HP Network Node Manager iSPI for IP Telephony Software

For the Windows® and Linux operating systems

Software Version: 10.00

Online Help

Document Release Date: July 2014

Software Release Date: July 2014

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

For information about third-party license agreements, see the license-agreements directory on the product installation media.

Copyright Notice

© Copyright 2008-2014 Hewlett-Packard Development Company, L.P.

Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, refer to the license-agreements directory on the NNMi product DVD.

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

This product includes ASM Bytecode Manipulation Framework software developed by Institute National de Recherche en Informatique et Automatique (INRIA). Copyright © 2000-2005 INRIA, France Telecom. All Rights Reserved.

This product includes Commons Discovery software developed by the Apache Software Foundation (http://www.apache.org/). Copyright © 2002-2008 The Apache Software Foundation. All Rights Reserved.

This product includes Netscape JavaScript Browser Detection Library software, Copyright © Netscape Communications 1999-2001

This product includes Xerces-J xml parser software developed by the Apache Software Foundation (http://www.apache.org/). Copyright © 1999-2002 The Apache Software Foundation. All rights reserved.

This product includes software developed by the Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). Xpp-3 Copyright © 2002 Extreme! Lab, Indiana University. All rights reserved.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Oracle Technology — Notice of Restricted Rights 3

Acknowledgements 4

Contents 8

HP Network Node Manager iSPI for IP Telephony Software 22

Chapter 1: Managing the IP Telephony Network 24

Chapter 2: Discovering IP Telephony Networks 26

Discover IP phones 26

Chapter 3: Help for Operators 27

IP Telephony Inventory 27

Acme IP Telephony 27

Monitoring Acme Session Directors 27

Filtering Session Directors 30

Session Director Details Form 31

Monitoring the Redundant Pair of a Session Director 32

Monitoring Realms 33

Realm Details Form 36

Monitoring Steering Pools 38

Steering Pool Details Form 41

Monitoring SIP Interfaces 41

SIP Interface Details Form 44

Monitoring SIP Ports 45

SIP Port Details Form 47

Monitoring Session Agent Statistics 48

Session Agent Statistics Details Form 51

Monitoring Session Agent Groups 52

Session Agent Group Details Form 56

Monitoring Network Interfaces 57

Network Interface Details Form 60

Viewing Discovered Acme Licenses 62

License Details Form 64

Viewing Discovered Acme Software 65
Acme SBC Software Details Form 67
Monitoring Configuration for Acme Session Director 67
Monitoring with Performance Graphs 68
Monitoring Realm Statistics 69
Enabling the Monitoring of Realm Statistics 70
Configuring the Realm Statistics Settings 72
Monitoring System Management Statistics 73
Enabling the Monitoring of System Management Statistics 74
Configuring the System Management Statistics Settings 75
Monitoring SIP Sessions 77
Enabling the Monitoring of SIP Sessions 78
Configuring the SIP Sessions Settings 79
Monitoring SIP Errors 82
Enabling the Monitoring of SIP Errors 83
Configuring the SIP Errors Settings 84
Monitoring SIP ACL Operations 88
Enabling the Monitoring of SIP ACL Operations 88
Configuring the SIP ACL Operations Settings 89
Monitoring SIP Transactions 92
Enabling the Monitoring of SIP Transactions 93
Configuring the SIP Transactions Settings 94
Monitoring SIP Client States 97
Enabling the Monitoring of SIP Client States 98
Configuring the SIP Client States Settings 99
Monitoring SIP Server States 102
Enabling the Monitoring of the SIP Server States 102
Configuring the SIP Server States Settings 103
Monitoring SIP Invites 106
Enabling the Monitoring of SIP Invites 106
Configuring the SIP Invites Settings 107

Monitoring Session Agents 110
Enabling the Monitoring of Session Agents 111
Configuring the Session Agents Settings 112
Avaya IP Telephony 115
Monitoring Avaya Call Controllers 115
Filtering Avaya Call Controllers 118
Avaya Call Controller Details Form 119
Monitoring Network Regions 122
Filtering Avaya Network Regions 123
IP Network Region Detail Form 124
Monitoring IP Media Processor DSP Resource Metrics 125
IP Network Region Connection Detail Form 127
Monitoring Route Patterns 128
Filtering Avaya Route Patterns 129
Route Pattern Details Form 130
Monitoring Trunk Group Usage 132
Monitoring Trunk Groups 133
Filtering Avaya Trunk Groups 134
Trunk Group Detailed Form 135
Monitoring Trunk Group Members 137
Trunk Group Member Detailed Form 138
Monitoring Signaling Groups 138
Signaling Group Details Form 139
Monitoring Processor Occupancy Metrics 140
Monitoring Avaya Port Networks 141
Filtering Avaya Port Networks 143
Port Network Detail Form 143
Monitoring IP Server Interface 144
IP Server Interface Details Form 146
Monitoring CLAN 147
CLAN Details Form 148

Monitoring Media Processors 149
Media Processor Details Form 152
Monitoring Port Network Load Details Metrics 154
Monitoring Total Load Metrics 155
Monitoring Intercom Load Metrics 155
Monitoring Incoming Trunk Load Metrics 155
Monitoring Outgoing Trunk Load Metrics 156
Monitoring Tandem Trunk Load Metrics 157
Monitoring Avaya IP Phones 157
Filtering Avaya IP phones 159
Avaya IP Phones Details Form 160
Monitoring Media Gateways 162
Filtering Avaya Media Gateways 164
Media Gateway Details Form 165
Monitoring Media Modules 167
Filtering Avaya Media Modules 168
Media Modules Form 169
Monitoring VOIP Engines 170
Filtering Avaya VOIP Engines 170
VOIP Engines Form 171
Monitoring DSP Cores 172
Filtering Avaya DSP Cores 173
DSP Cores Form 174
Cisco IP Telephony 175
Monitoring Cisco Unified Communications Manager Clusters 175
Filtering UCM Clusters 178
UCM Cluster Details Form 179
Monitoring UCM Subscriber Groups 180
UCM Subscriber Group Details Form 183
Monitoring Cisco Unified Communications Managers 183
Cisco Call Controller Details Form 187

Monitoring Device Pools ... 191
Device Pool Details Form ... 194
Monitoring H.323 Gateways ... 195
Viewing Cisco Voice Gateway Details Form ... 199
Monitoring MGCP/SCCP Gateways ... 200
Voice Gateway Interface Details Form ... 204
Voice Gateway Channels Details Form ... 207
Monitoring SRST Routers ... 208
Cisco Call Controller Details Form ... 211
Monitoring H323 Trunks ... 215
H323 Trunk Details Form ... 218
Monitoring SIP Trunks ... 219
SIP Trunk Details Form ... 220
Monitoring NTP Servers ... 221
NTP Server Details Form ... 222
Monitoring Media Devices ... 223
Media Device Details Form ... 225
Monitoring Voice Mail Devices ... 226
Monitoring Locations ... 227
Location Details Form ... 229
Monitoring UCMEs ... 230
Filtering UCMEs ... 231
Cisco Call Controller Details Form ... 232
Monitoring IP Phones ... 236
Filtering Cisco IP phones ... 239
Cisco Extension Details form ... 240
Updating Site Codes, Mail Codes, and Location Details of Cisco IP Phones ... 242
Monitoring Cisco Gatekeepers ... 244
Filtering Cisco Gatekeepers ... 245
Cisco GateKeeper Details Form ... 246
Monitoring Voice Gateways ... 246

Analysis Pane 248
Voice Gateway Summary tab 248
Voice Gateway Information tab: 248
Voice Gateway Interface Details tab: 248
Filtering Cisco Voice Gateways 249
Filtering Voice Gateway Interfaces 250
Viewing Cisco Voice Gateway Endpoint Channels 251
Analysis Pane 252
Voice Gateway Channels Summary tab 252
Cisco VGW Channel Information tab 252
Monitoring Cisco Unity Devices 252
Filtering Cisco Unity Devices 253
Cisco Unity Devices Form 254
Monitoring Configuration for Cisco Unified Communications Manager Clusters and Cisco Unified Communications Managers 254
Guidelines 255
Monitoring UCM Call Activities 255
Enabling the Monitoring of UCM Call Activity 256
Configuring the UCM Call Activity Settings 258
Monitoring Registered Devices Count 260
Enabling the Monitoring of Registered Devices Count 261
Configuring the Registered Devices Count Settings 262
Monitoring Gateway Call Activity 266
Enabling the Monitoring of Gateway Call Activity 266
Configuring the Gateway Call Activity Settings 269
Monitoring Route List and Hunt List Count Configurations 271
Enabling the Monitoring of Route List and Hunt List Count Configurations 271
Configuring the Route List and Hunt List Count Settings 272
Monitoring Media Resource Activity 275
Enabling the Monitoring of Media Resource Activity 275
Configuring the Media Resource Activity Settings 277
Monitoring CTIManager Connections Count 279

Enabling the Monitoring of CTIManager Connections Count 279
Configuring the CTIManager Connections Count Settings 281
Monitoring Locations 283
Enabling the Monitoring of Locations 283
Configuring the Locations Settings 285
Monitoring SIP Trunk Sessions 286
Enabling the Monitoring of SIP Trunk Sessions 287
Configuring the SIP Trunk Sessions Settings 288
Monitoring RAID Status 290
Enabling the Monitoring of RAID Status 290
Configuring the RAID Status Settings 292
Monitoring the Cisco TFTP Server 293
Enabling the Monitoring of Cisco TFTP Server 295
Configuring the Cisco TFTP Server Settings 296
Monitoring the Health of Cisco Unified Communications Managers 299
Enabling the Monitoring of System Health Parameters 299
Configuring the System Health Parameter Settings 301
Monitoring the Availability of the Call Manager Administration Web Page 304
Enabling the Monitoring of the Call Manager Administration Web Page State 304
Configuring the Call Manager Administration Web Page State Settings 305
Monitoring the Availability of Services on the UCM 306
Enabling the Monitoring of the Availability of Services on the UCM 307
Configuring the Availability of Services on the UCM Settings 308
ClarusIPC Integration–Test Plans and Test Result Reports 309
Viewing Route Group P.01 Grade of Service Summary Report 310
Viewing Route List P.01 Grade of Service Summary Report 312
Microsoft IP Telephony 314
Monitoring Lync Sites 314
Viewing the Analysis Panel for a Quick Reference 315
Launching Context-sensitive Actions for a Lync Site 316
Lync Sites Form 317

Pool Form 318
Monitoring End User Groups 319
Viewing the Analysis Panel for a Quick Reference 319
Launching Context-sensitive Actions for a Lync End User Group 320
End User Group Form 320
Monitoring End Users 321
Launching Context-sensitive Actions for a Lync End User 322
Lync End User Form 322
Active Endpoints Form 325
Monitoring Lync Servers 325
Servers Form 326
Monitoring Gateways 327
Launching Context-Sensitive Reports for a Gateway 328
Analysis Pane 329
Gateway Form 329
Gateway Interface Form 332
Gateway Channel Form 334
Monitoring SIP Trunk Configurations 336
SIP Trunk Configuration Form 337
Monitoring Dial Plans 338
Dial Plan Form 339
Normalization Rule Form 340
Monitoring Voice Routes 341
Voice Routes Form 342
Monitoring Voice Policies 343
Voice Policy Form 343
Monitoring Sites 345
Launching Context-sensitive Actions for a Site 345
Sites Form 346
Viewing the Lync Enterprise Map 346
Saved Lync Maps 348

Launching Saved Maps 349
Deleting Saved Maps 349
Health Indicator Form 350
Filtering Central Sites 351
Nortel IP Telephony 352
Monitoring Nortel Call Servers 352
Filtering Nortel Call Servers 354
Nortel Call Server form 355
Monitor Nortel Signaling Servers 355
Filtering Nortel Signaling Servers 357
Nortel Signaling Server Details Form 358
Nortel QOS Zones Table View 359
View the Nortel QOS Zone Details form 359
Filtering Nortel QOS Zones 360
View the Nortel QOS Zone Details Form 360
Nortel IP Phones View 362
Filtering Nortel IP phones 363
Nortel Phone Detailed form 364
Monitoring Nortel Media Gateways 365
Filtering Nortel Media Gateways 366
View the Nortel Media Gateway Details Form 366
Incidents Collected from the ClarusIPC Environment 367
Context-Sensitive URLs for ClarusIPC Incidents 368
Incidents Generated by the NNM iSPI for IP Telephony 369
View SNMP Traps for Avaya Maintenance Objects 410
Incidents for Avaya Devices 411
Viewing Network Connectivity 412
Viewing the Graph for Jitter 414
Viewing the Graphs for Average Packet Loss 414
Viewing the Graph for the Average MOS 415
Viewing the Graphs for Latency 416

Launch a Voice Path 416
Launch a Control Path 417
Launch the HTTP to Phone Path 418
Integration with the iSPI Performance for Quality Assurance 419
Integration with the iSPI Performance for Traffic 419
Chapter 5: Help for Administrators 422
Acme IP Telephony 424
Configuring Call Monitoring 424
Configuring the QOS/MOS Threshold Values for Call Monitoring 425
Configuring Session Director—specific QOS and MOS Threshold Values 426
Configuring the Call Termination Cause Codes to be Monitored 427
Configuring Data Access 429
Accessing the Acme Session Director with SSH 429
Accessing the CDR Data 430
Accessing the HDR Data for Acme Session Director 435
Configuring Polling 437
Configuring Reporting 438
Avaya IP Telephony 438
Configuring Call Monitoring 439
Configuring the QOS/MOS Threshold Values for Call Monitoring 439
Configuring Communication Manager—specific QOS and MOS Threshold Values 440
Configuring the Call Termination Cause Codes to be Monitored 442
Configuring Data Access 443
Accessing the CDR Data 444
Configuring RTCP Reception 450
Configuring SSH Access 453
Configuring Discovery Settings for Avaya Primary Servers 454
Configuring Discovery Cycle for Avaya Primary Servers 454
Configuring IP Phones 456
Specifying the Range of Extensions for Avaya Phones to be Excluded from Monitoring 457

Specifying the List of IP Phones for Registration State Change Incident Generation 458
Configuring Custom Attribute Settings for the IP Phones 459
Configuring Polling 460
Configuring the Polling of a Communication Manager 460
Configuring the Polling of a Media Gateway 464
Configuring Reporting 465
Configuring CDR Reporting 466
Enabling Phone MAC Reports 466
Enabling Trunk Activity Reports 469
Enabling Trunk Group Usage Reports 469
Enabling Processor Occupancy Summary Reports 469
Enabling Port Network Load Reports 470
Enabling IP Network Region DSP/Codec Summary Report 470
Enabling Route Pattern Usage Report 471
Cisco IP Telephony 471
Configuring the Call Monitoring 472
Configuring the QOS and MOS Monitoring Threshold Values for Cisco 472
Configuring Cluster-specific QOS and MOS Monitoring Threshold Values 473
Configuring Call Termination Cause Codes to be Monitored 475
Configuring Data Access 476
Configuring the NNM iSPI for IP Telephony to Access the AXL Data 476
Accessing the CDR Data 479
Accessing the Cisco Unified Communications Manager with SSH 485
Configuring Discovery Settings for Cisco H.323 Gateways 487
Configuring IP Phones 488
Specifying the Range of Extensions for Cisco Phones to be Excluded from Monitoring 489
Specifying the List of IP Phones for Registration State Change Incident Generation 490
Configuring Custom Attributes Settings for Cisco IP Phones 491
Configuring Polling 492

Configuring Polling that is Specific to Cisco Unified Communications Manager 492
Configuring Polling that is Specific to Cisco Survivable Remote Site Telephony (SRST) Routers 494
Configuring Polling that is Specific to Cisco Gatekeepers 494
Configuring Polling that is Specific to Unity Devices and Unity Connection Servers 495
Configuring Polling that is Specific to Cisco Voice Gateways 496
Configure Reporting 497
Configuring CDR Reporting 497
Enabling Cisco B-Channel Activity Reports 498
Enabling Phone MAC Reports 498
Enabling Voice Mail Reports 500
Microsoft IP Telephony 502
Configuring Call Monitoring 503
Configuring Threshold Values for the Monitoring of QoE 503
Configuring Site-specific Threshold Values for the Monitoring of QoE 504
Configuring the Call Termination Cause Codes to be Monitored 507
Configuring Frontend Server Communication 508
Adding a New Front End Server Communication Configuration 509
Configuring Gateway 510
Configuring Gateway Interface State Polling 511
Configuring Gateway Channel State Polling 512
Configuring Gateway Performance Data Collection 513
Configuring Lync End Users 514
Creating End User Groups 515
Adding a New Lync End User Group 515
Creating Named End User Groups 519
Creating Excluded End User Groups 520
Configuring Periodic Collection 521
Configuring Call Detail Record Collection 522
Configuring Quality of Experience Collection 523
Configuring Topology Discovery Details 523

Configuring User Discovery Details 524
Configuring MS IPT Proxy with NNM iSPI for IP Telephony 525
Adding a New Proxy Communication Configuration 526
Configuring Sites 527
Adding a New Site Configuration 528
Integrating with SiteScope 531
Integration Considerations 532
Enabling Performance Monitoring for Microsoft Unified Communication and Collaboration Applications 532
Nortel IP Telephony 533
Configuring Data Access 533
Configuring IP Phones 535
Specifying the Range of Extensions for Nortel Phones to be Excluded from Monitoring 535
Specifying the List of IP Phones for Registration State Change Incident Generation 537
Configuring Polling 537
Extracting a Host Key 538
Global IP Telephony Network Management 542
Configuration Points 543
Regional Manager Configuration 543
Adding a Regional Manager Configuration 544
Modifying a Regional Manager Configuration 546
Deleting a Regional Manager Configuration 546
Importing Configuration from the Regional Manager to the Global Manager 547
Managing the Lifecycle of NNMi Nodes Hosting IP Telephony Devices 548
Managing Cisco IP Telephony Devices 549
Managing Avaya IP Telephony Devices 552
Deleting IP Telephony Entities from the NNM iSPI for IP Telephony 555
Configuring Processing of Traps Sent by Nortel Call Server 556
NNM iSPI for IP Telephony Logging 557
To set the logging level, follow these steps: 557

Integration with ClarusIPC 559

We appreciate your feedback! 561

HP Network Node Manager iSPI for IP Telephony Software

The HP Network Node Manager iSPI for IP Telephony Software (**NNM iSPI for IP Telephony**) extends the capability of NNMi to monitor and manage the IP telephony infrastructure in your network environment. The NNM iSPI for IP Telephony presents additional views to indicate the states of discovered IP telephony devices and display the overall health of the IP telephony infrastructure.

The NNM iSPI for IP Telephony, in conjunction with NNMi, performs the following tasks:

- Automatic discovery of the IP telephony infrastructure
- Display the IP telephony devices in the IP telephony views
- Monitor the status of every discovered component of the IP telephony infrastructure

After you install (and configure) the NNM iSPI for IP Telephony on the NNMi management server, you can monitor and troubleshoot the problems in your IP telephony infrastructure with the additional views provided by the NNM iSPI for IP Telephony.

Chapter 1: Managing the IP Telephony Network

The NNM iSPI for IP Telephony provides you with a complete framework to monitor the IP telephony devices available on your network. You can discover all the available IP telephony devices and topologies with the help of the NNM iSPI for IP Telephony. After installing and configuring the NNM iSPI for IP Telephony, you can perform the following tasks:

- **Monitoring the states of the IP telephony environment**
  The inventory views presented by the NNM iSPI for IP Telephony shows detailed states of every discovered device in tables. You can view the following details of a device:
  - IP address and hostname
  - Version, model, or type of the device
  - Status of the device
- **Monitoring the health of the IP telephony network**
  The IP Telephony network consists of several IP telephony devices along with several networking devices and elements. The NNM iSPI for IP Telephony can identify the faults related to IP telephony communication on the network topology that is discovered by NNMi. NNMi, in conjunction with the NNM iSPI for IP Telephony, presents the faults identified in the discovered topology in the network inventory views.
- **Investigating problems and troubleshooting**
  NNMi helps you view the discovered network topology in a graphical format, which assists you in diagnosing the defects in your network. You can view the layer 2 or layer 3 path for every device. You can also view the connectivity status between two or more devices. Each device is represented as a node in these graphs, and the color of each node indicates the status of the device.

Chapter 2: Discovering IP Telephony Networks

You can start monitoring all the IP telephony infrastructure after a cycle of polling by the NNM iSPI for IP Telephony. You can install the NNM iSPI for IP Telephony for an IP telephony network that is already being managed by NNMi, or you can configure NNMi to monitor an IP telephony network after the installation of the NNM iSPI for IP Telephony.

If you install the NNM iSPI for IP Telephony on an NNMi management server that is already managing an IP telephony network, the subsequent NNMi discovery prompts the NNM iSPI for IP Telephony to discover the IP telephony devices and topologies. Completion of the NNMi discovery cycle always triggers the discovery of the IP telephony network by the NNM iSPI for IP Telephony. By default, the NNMi and NNM iSPI for IP Telephony discovery schedule is set to 24 hours.

After installing the NNM iSPI for IP Telephony to monitor an IP telephony network that was already being managed by NNMi, you can wait for the next discovery cycle of NNMi, or you can run the Configuration Poll action to discover the IP telephony network immediately.

If you install the NNM iSPI for IP Telephony to monitor a network, which is not already managed by NNMi, you must seed all the IP telephony devices from the NNMi console after installation. Seeding enables NNMi to perform Configuration Poll and triggers a cycle of discovery. In effect, the IP telephony network is discovered at the end of the discovery cycle.

Discover IP phones

As IP phones are not SNMP-enabled devices, a standard discovery by the NNM iSPI for IP Telephony cannot discover these phones. To discover IP phones available in your network, you must do the following:

- Seed the access switches to which the IP phones are connected
- Set up auto-discovery rules for IP phones
- Disable ping sweep while setting up auto-discovery for IP phones

The auto-discovery rule discovers the IP telephony network including layer 2 connections between IP phones on the network.

Chapter 3: Help for Operators

To perform a basic monitoring of the IP Telephony network, you can log on to the NNMi console with the operator (level 1 or 2) or guest credentials. After you log on to the NNMi console, you can view the inventory views introduced by the NNM iSPI for IP Telephony. You can access the views to monitor the status and necessary details for every IP Telephony device.

IP Telephony Inventory

The NNM iSPI for IP Telephony provides the following workspaces to the NNMi console:

- **Acme IP Telephony**
- **Cisco IP Telephony**
- **Avaya IP Telephony**
- **Nortel IP Telephony**
- **Microsoft IP Telephony**

You can access all the IP Telephony–related views from these workspaces. The individual views present the device details in tables, and you can launch forms from the views to access the connectivity details.

To launch an IP telephony view, follow these steps:

1. From the Workspaces pane, click the IP Telephony tab that you want to view. The selected IP Telephony tab expands and displays the available IP Telephony view.
2. Click the view of your interest. The view appears on the right pane.

In this document, the Cisco Unified Communication Manager server is referred to as the Cisco CallManager server.

Acme IP Telephony

The Acme IP Telephony workspace enables you to view the inventory of the Acme Session Directors (SDs) that are discovered and monitored in your environment.

Monitoring Acme Session Directors

The Acme Session Director view displays the details of the Acme Session Directors discovered on the network. The view arranges the key attributes of all the discovered Acme Session Directors in a table.

To launch the Acme Session Director view, follow this step:

- From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Acme Session Director view opens in the right pane.

Basic Attributes of the Session Director Table

Attribute	Description
State	Indicates the redundancy state of the Acme Session Director. The state can be one of the following: ▪ Unknown - indicates that the status of the Session Director is currently unknown. ▪ Initial - indicates that the Session Director is in the initial state. ▪ Active - indicates the Session Director is in the active state. ▪ Standby - indicates that the Session Director is in the standby state. ▪ Out Of Service - indicates that the Session Director is currently out of service. ▪ Not Monitored - indicates that the Session Director is not monitored.
Name	Indicates the name of the Acme Session Director.
IP Address	Indicates the IP address of the Acme Session Director.
Tenant	Indicates the name of the tenant to which the Acme Session Director belongs.
Description	A brief description of the Acme Session Director.
Management Server	The management server for the Acme Session Director. This attribute displays one of the following values: ▪ **Local**: If the Session Director is being managed by the NNMi management server console on which you are viewing the Session Director details. ▪ Name of the regional manager that manages the Session Director.

Session Director Details Form

You can view the details of the discovered Session Directors using the Session Director Details form.

To view the Session Director Details form, follow this step:

- From the Acme Session Director view table, select the Session Director for which you want to view the details, and then click . The Session Director Details form opens.

Analysis Pane

You can view a summary of the details of the selected Session Director on the Analysis pane. The following tabs and related details are displayed:

- **Session Director Details Summary Tab**
  - Name: The name of the selected Session Director.
  - Management Address: The IP address of the selected Session Director.
  - Tenant: The name of the tenant to which the selected Session Director belongs.
  - Management Server: The management server for the selected Session Director. This attribute displays one of the following values:
    - **Local**: If the Session Director is being managed by the NNMi management server console on which you are viewing the Session Director details.
    - Name of the regional manager that manages the Session Director.
- **Session Director Information Tab**
  - Management Mode: The management status of the selected Session Director. The status can be one of the following:
    - Managed: indicates that the Session Director is managed by NNM iSPI for IP Telephony
    - Out of Service: indicates that the Session Director is currently out of service and is not managed by NNM iSPI for IP Telephony
    - Unmanaged: indicates that the Session Director is not managed by NNM iSPI for IP Telephony
  - IP Address: The IP address of the selected Session Director.
  - Description: A brief description of the selected Session Director.
  - Redundancy State: The redundancy state of the selected Session Director. The state can be one of the following:
    - Unknown - indicates that the status of the Session Director is currently unknown.
    - Initial - indicates that the Session Director is in the initial state.
    - Active - indicates the Session Director is in the active state.
    - Standby - indicates that the Session Director is in the standby state.
    - OutOfService - indicates that the Session Director is currently out of service.
  - Current configuration version: The current configuration version of the selected Session Director.
  - Running configuration version: The running configuration version of the selected Session Director.
  - Backup configuration: The backup configuration details of the selected Session Director.
  - Custom Info: The custom information configured for the selected Session Director.

- **Realm Statistics Tab**
  Displays the details of the measurement attributes configured for the Realm. For more information about the measurement attributes configured for Realms, see Monitoring Realm Statistics.

- **SIP ACL Operations Tab**
  Displays the details of the measurement attributes configured for the SIP ACL Operations. For more information about the measurement attributes configured for SIP ACL Operations, see Monitoring SIP ACL Operations.

- **SIP Client States Tab**
  Displays the details of the measurement attributes configured for the SIP Client States. For more information about the measurement attributes configured for SIP Client States, see Monitoring SIP Client States.

- **SIP Errors Tab**
  Displays the details of the measurement attributes configured for the SIP Errors. For more information about the measurement attributes configured for SIP Errors, see Monitoring SIP Errors.

- **SIP Invites Tab**
  Displays the details of the measurement attributes configured for the SIP Invites. For more information about the measurement attributes configured for SIP Invites, see Monitoring SIP Invites.

- **SIP Server States Tab**
  Displays the details of the measurement attributes configured for the SIP Server States. For more information about the measurement attributes configured for SIP Server States, see Monitoring SIP Server States.

- **SIP Sessions Tab**
  Displays the details of the measurement attributes configured for the SIP Sessions. For more information about the measurement attributes configured for SIP Sessions, see Monitoring SIP Sessions.

- **SIP Transactions Tab**
  Displays the details of the measurement attributes configured for the SIP Transactions. For more information about the measurement attributes configured for SIP Transactions, see Monitoring SIP Transactions.

- **System Tab**
  Displays the details of the measurement attributes configured for the System Management. For more information about the measurement attributes configured for System Management, see Monitoring System Management Statistics .

Filtering Session Directors

You can filter the Session Directors, listed in the **Session Directors** view, using the available filters. This feature enables you to view the Session Directors based on the filter option that you

selected. You can perform the filtering action on all the columns available on the Session Director view table.

Note: You can select multiple filters based on your requirements.

To filter the Acme Session Directors view, follow these steps:

1. Select a Session Director, listed in the **Session Directors** view, and right-click one of the following column attributes:
   - **State**
   - **Name**
   - **IP Address**
   - **Tenant**
   - **Description**
   - **Management Server**
2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the Session Directors that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the Session Directors for which the selected column is not empty.
   - **Is empty**: filters and lists all the Session Directors for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the Session Directors that do not have the value in the column that you selected.

The filtered list of the Session Directors appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Session Director Details Form

The Session Director Details form is split into two panes. The left pane displays the general and SBC HA Node attributes of the selected Session Director.

General

- Hosted Node: The node on which the Session Director is hosted.
- Name: The name of the Session Director.
- State: The redundancy state of the Session Director.
- IP Address: The IP address of the Session Director.
- Tenant: The name of the tenant to which the Session Director belongs.
- Description: A brief description of the Session Director.
- Custom Info: The custom information configured for the Session Director. This attribute displays *Not Set* if you have not specified the custom information. To specify a custom information for the Session Director, type the required information, and then click (the **Save** icon).

SBC HA Node

- Peer Name: The peer name of the Session Director. For a Session Director in Active state, this field displays the name of the Session Director in Standby state and vice versa.
- HA State: The state of the HA node.

The right pane displays the following tabs:

- Redundant Pair
- Realms
- Session Agent Statistics
- Session Agent Groups
- Network Interface
- License
- Software

The Session Director Details form also displays the **Analysis Pane** at the bottom. This pane displays a summary of the details of the selected Session Director. For more information, see Monitoring Acme Session Directors.

Monitoring the Redundant Pair of a Session Director

The Redundant Pair view displays the details of the redundant pair of a selected Session Director. For example, for an SD in the **Active** state, this view displays the SD that is in the **Standby** state and vice versa. The view arranges the key attributes of the Redundant Pair in a table.

To launch the Redundant Pair view, follow these steps:

1. From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Session Director view opens on the right pane.
2. Select the Session Director for which you want to launch the Redundant Pair view, and then click . The Session Director Details form opens.
3. On the right pane of the form, click the **Redundant Pair** tab. The Redundant Pair view opens.

Basic Attributes of the Redundant Pair Table

Attribute	Description
State	Indicates the state of the redundant pair.
Name	Indicate the name of the Session Director.
IP Address	Indicates the IP address of the Session Director.
Tenant	Indicates the tenant to which the Session Director belongs.
Description	Indicates a brief description of the Session Director.
Management Server	Indicates the management server for the selected Session Director. This attribute displays one of the following values: • **Local**: If the Session Director is being managed by the NNMi management server console on which you are viewing the Session Director details. • Name of the regional manager that manages the Session Director.

Viewing the Redundant Session Director Details

You can view the details of the selected redundant pair of the Session Director using the Session Director Details form.

To view the Session Director Details form, follow this step:

- From the Redundant Pair view table, select the redundant pair of the Session Director to view the details, and then click . The Session Director Details form opens.

Analysis Pane

You can view a summary of the details of the selected redundant pair of the Session Director on the Analysis pane. For more information about the Analysis Pane of the Session Director Details form, see Monitoring Acme Session Directors.

Monitoring Realms

The Realms view displays the details of the Realms associated with a Session Director. The view arranges the key attributes of the Realms in a table.

To launch the Realms view, follow these steps:

1. From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Session Director view opens on the right pane.
2. Select the Session Director for which you want to launch the Realm view, and then click . The Session Director Details form opens.
3. On the right pane of the form, click the **Realms** tab. The Realms view opens.

Basic Attributes of the Realms Table

Attribute	Description
Status	Indicates the status of the Realm. The status can be one of the following: • Unknown • InService • ConstraintsViolation • CallLoadReduction
Identifier	Indicates the name of the Realm.
Description	Indicates a brief description of the Realm configuration.

Realm Details Form

You can view the details of the selected Realm using the Realm Details form.

To view the Realm Details form, follow this step:

- From the Realms view table, select the Realm for which you want to view the details, and then click . The Realm Details form opens.

Filtering Realms

You can filter the Realms, listed in the Realms view, using the available filters. This feature enables you to view the Realms based on the filter option that you selected. You can perform the filtering action on all the columns available on the Realm view table.

Note: You can select multiple filters based on your requirements.

To filter the Realms view, follow these steps:

1. Select a Realm, listed in the Realms view, and right-click one of the following column attributes:
   - **Status**
   - **Identifier**

- **Description**

2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the Realms that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the Realms for which the selected column is not empty.
   - **Is empty**: filters and lists all the Realms for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the Realms that do not have the value in the column that you selected.

The filtered list of the Realms appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected Realm on the Analysis pane. The following tabs and related details are displayed:

- **Realm Details Summary Tab**
  - Identifier: The name of the selected Realm.
  - Status: Indicates the status of the Realm. The status can be one of the following:
    - Unknown
    - In Service
    - ConstraintsViolation
    - CallLoadReduction
  - Tenant: The name of the tenant to which the selected Realm belongs.
  - Management Server: The management server for the selected Realm. This attribute displays one of the following values:
    - **Local**: If the Realm is being managed by the NNMi management server console on which you are viewing the Realm details.
    - Name of the regional manager that manages the Realm.
- **Realm Information Tab**
  - Description: A brief description of the Realm configuration.
  - Addr-prefix: The IP address prefix of the address associated with the Realm.

- Media-policy: The media-policy element that applies to the flow of the Realm.
- Class-Profile: The class-profile used for the Realm.
- Last-modified-by: The user who modified the Realm configuration.
- Last-modified-date: The date and time when the configuration of the Realm was last modified.

- **Realm Statistics Tab**
  - Inbound Current Active Sessions: Number of active inbound sessions for the Realm.
  - Inbound Current Session Rate: Call per second (CPS) rate of active inbound sessions for the Realm.
  - Outbound Current Active Sessions: Number of active outbound sessions for the Realm.
  - Outbound Current Session Rate: CPS rate of active outbound sessions for the Realm.
  - Inbound Total Sessions: Total number of inbound sessions for the Realm.
  - Outbound Total Sessions: Total number of outbound sessions for the Realm.

Realm Details Form

The Realm Details form is split into two panes. The left pane displays the following details:

- General
- Realm Service Profile

The right pane displays the following tabs:

- Session Agent Statistics
- Steering Pool
- SIP Interfaces
- Network Interface

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
Identifier	Indicates the name of the Realm.
Description	Indicates a brief description of the Realm configuration.

Attribute	Description
Status	Indicates the status of the Realm. The status can be one of the following: • Unknown • InService • ConstraintsViolation • CallLoadReduction
Addr-prefix	Indicates the IP address prefix of the address associated with the Realm.
Media-policy	Indicates the media-policy element that applies to the flow of the Realm.
Class-profile	Indicates the class-profile used for the Realm.
Constraint-name	Indicates the name of the constraint used for the Realm.
In-translationid	Indicates the identifier/name of the session-translation element that applies to the incoming addresses for the Realm.
Out-translationid	Indicates the identifier/name of the session-translation element that applies to the outgoing addresses for the Realm.
Network-interfaces	Indicates the Network Interfaces through which the Realm can be reached.
Refer-call-transfer	Indicates whether the refer-call-transfer feature for the Realm is enabled or disabled.
In-manipulationid	Indicates the inbound SIP manipulation rule name.
Out-manipulationid	Indicates the outbound SIP manipulation rule name.
Last-modified-by	Indicates the user who modified the Realm configuration.
Last-modified-date	Indicates the date and time when the configuration of the Realm was last modified.

Realm Service Profile

The attributes that appear under the **Realm Service Profile** section are described in the following table:

Attribute	Description
Max-bandwidth	Indicates the total bandwidth budget per second for all flows to and from the Realm.
Mm-in-Realm	Indicates whether the parameter to treat media within the Realm is enabled or disabled.
Mm-in-network	Indicates whether the parameter to treat media in Realms with the same subnet mask is enabled or disabled.
Msm-release	Indicates whether the media release information of multiple Session Directors, included in the SIP signaling request sent to the Realm, is enabled or disabled.

Session Agents

The **Session Agents** tab lists all the Session Agents associated with the Realm. You can select a Session Agent from the list displayed by the **Session Agents** tab, and click to open the Session Agent Statistics Details form and view the details of the specific Session Agent.

Steering Pool

The **Steering Pool** tab lists the Steering Pool associated with the Realm. You can select a Steering Pool from the list displayed by the **Steering Pool** tab, and click to open the Acme SBC Steering Pool Details form and view the details of the specific Steering Pool.

SIP Interfaces

The **SIP Interfaces** tab lists the Session Initiation Protocol (SIP) Interfaces associated with the Realm. You can select a SIP Interface from the list displayed by the **SIP Interface** tab, and click to open the Acme SBC SIP Interface Details form and view the details of the specific SIP interface.

Network Interfaces

The **Network Interfaces** tab lists the assigned Network Interfaces associated with the Realm. You can select a Network Interface from the list displayed by the **Network Interface** tab, and click to open the Acme SBC Network Interface Details form and view the details of the specific Network Interface.

Analysis Pane

The Analysis pane displays a summary of the details of the selected Realm. For more information, see Monitoring Realms.

Monitoring Steering Pools

The Steering Pool view on the right pane of the Realm Details form displays the details of the Steering Pool associated with a Realm. The view arranges the key attributes of the Steering Pool in a table.

To launch the Steering Pool view, follow these steps:

1. From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Session Director view opens on the right pane.
2. Select the Session Director for which you want to launch the Realm view, and then click . The Session Director Details form opens.
3. On the right pane of the form, click the **Realms** tab. The Realms view opens.
4. Select the Realm for which you want to launch the Steering Pool view, and then click . The Realm Details form opens.
5. On the right pane of the form. click the **Steering Pool** tab. The Steering Pool view opens.

Basic Attributes of the Steering Pool Table

Attribute	Description
IP Address	Indicates the IPv4 address of the Steering Pool.
RealmID	Indicates the ID of the Realm of the Steering Pool.
Start Port	Indicates the port number that begins the range of ports available in the Steering Pool.
End Port	Indicates the port number that ends the range of ports available in the Steering Pool.

Acme SBC Steering Pool Details Form

You can view the details of the selected Steering Pool using the Acme SBC Steering Pool Details form.

To view the Acme SBC Steering Pool Details form, follow this step:

- From the Steering Pool view table, select the Steering Pool for which you want to view the details, and then click . The Acme SBC Steering Pool Details form opens.

Filtering Steering Pools

You can filter the Steering Pools, listed in the Steering Pool view, using the available filters. This feature enables you to view the Steering Pools based on the filter option that you selected. You can perform the filtering action on all the columns available on the Steering Pool view table.

Note: You can select multiple filters based on your requirements.

To filter the Steering Pools view, follow these steps:

1. Select a Steering Pool, listed in the Steering Pool view, and right-click one of the following column attributes:

- **IP Address**
- **Realm ID**
- **Start Port**
- **End Port**

2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the Steering Pools that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the Steering Pools for which the selected column is not empty.
   - **Is empty**: filters and lists all the Steering Pools for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the Steering Pools that do not have the value in the column that you selected.

The filtered list of the Steering Pools appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected Steering Pool on the Analysis pane. The following tabs and related details are displayed:

- **Acme SBC Steering Pool Details Summary Tab**
  - IP Address: The IPv4 address of the Steering Pool.
  - Realm-id: The ID of the Realm of the Steering Pool.
  - Tenant: The name of the tenant to which the selected Steering Pool belongs.
  - Management Server: The management server for the selected Steering Pool. This attribute displays one of the following values:
    - **Local**: If the Steering Pool is being managed by the NNMi management server console on which you are viewing the Steering Pool details.
    - Name of the regional manager that manages the Steering Pool.
- **Steering Pool Information Tab**
  - Start Port: The port number that begins the range of ports available in the Steering Pool.
  - End Port: The port number that ends the range of ports available in the Steering Pool.

- Last-modified-by: The user who last modified the configuration of the Steering Pool.
- Last-modified-date: The date and time when the configuration of the Steering Pool was last modified.

Steering Pool Details Form

The Steering Pool Details form displays the general attributes of the Steering Pool.

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
IP Address	Indicates the IPv4 address of the Steering Pool.
Realm ID	Indicates the ID of the realm of the Steering Pool.
Start Port	Indicates the port number that begins the range of ports available in the Steering Pool.
End Port	Indicates the port number that ends the range of ports available in the Steering Pool.
Network Interface	Indicates the network interface towards which the Steering Pool directs its media.
Last Modified By	Indicates the name of the user who last modified the configuration of the Steering Pool.
Last Modified Date	Indicates the date and time when the configuration of the Steering Pool was last modified.

Analysis Pane

The Analysis pane displays a summary of the details of the selected Steering Pool. For more information, see Monitoring Steering Pools.

Monitoring SIP Interfaces

The SIP Interfaces view on the right pane of the Realm Details form displays the details of the SIP Interface associated with a Realm. The view arranges the key attributes of the SIP Interfaces in a table.

To launch the SIP Interfaces view, follow these steps:

1. From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Acme Session Director view opens on the right pane.

2. Select the session director for which you want to launch the Realm view, and then click . The Session Director Details form opens.
3. On the right pane of the form, click the **Realms** tab. The Realms view opens.
4. Select the Realm for which you want to launch the SIP Interfaces view, and then click . The Realm Details form opens.
5. On the right pane of the form. click the **SIP Interfaces** tab. The SIP Interfaces view opens.

Basic Attributes of the SIP Interfaces Table

Attribute	Description
State	Indicates the state of the SIP Interface. The state can be one of the following: • Enabled: Indicates that the SIP Interface connected to the Realm is enabled. • Disabled: Indicates that the SIP Interface connected to the Realm is disabled.
Description	A brief description of the SIP Interface associated with the Realm.

Acme SBC SIP Interface Details Form

You can view the details of the selected SIP Interface using the Acme SBC SIP Interface Details form.

To view the Acme SBC SIP Interface Details form, follow this step:

- From the SIP Interface view table, select the SIP Interface for which you want to view the details, and then click . The Acme SBC SIP Interface Details form opens.

Filtering SIP Interfaces

You can filter the SIP Interfaces, listed in the SIP Interface view, using the available filters. This feature enables you to view the SIP Interfaces based on the filter option that you selected. You can perform the filtering action on all the columns available on the SIP Interfaces view table.

Note: You can select multiple filters based on your requirements.

To filter the SIP Interfaces view, follow these steps:

1. Select a SIP Interface, listed in the SIP Interface view, and right-click one of the following column attributes:
   - **State**
   - **Description**

2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the SIP Interfaces that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the SIP Interfaces for which the selected column is not empty.
   - **Is empty**: filters and lists all the SIP Interfaces for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the SIP Interfaces that do not have the value in the column that you selected.

The filtered list of the SIP Interfaces appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected SIP Interface on the Analysis pane. The following tabs and related details are displayed:

- **Acme SBC SIP Interface Details Summary Tab**
  - Description: A brief description of the SIP Interface.
  - Management Server: The management server for the selected SIP Interface. This attribute displays one of the following values:
    - **Local**: If the SIP interface is being managed by the NNMi management server console on which you are viewing the SIP Interface details.
    - Name of the regional manager that manages the SIP Interface.
- **SIP Interface Information Tab**
  - State: Indicates the state of the SIP Interface. The state can be one of the following:
    - Enabled: Indicates that the SIP Interface connected to the Realm is enabled.
    - Disabled: Indicates that the SIP Interface connected to the Realm is disabled.
  - Realm-id: Indicates the name of the Realm to which the SIP Interface is connected.
  - Last-modified-by: Indicates the name of the user who last modified the configuration of the SIP Interface.
  - Last-modified-date: The date and time when the configuration of the SIP Interface was last modified.

SIP Interface Details Form

The SIP Interface Details form is split into two panes. The left pane displays the general attributes of the SIP Interface. The right pane displays the following tabs:

- SIP Ports
- Network Interfaces

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
Description	A brief description of the SIP Interface associated with the Realm.
State	Indicates the state of the SIP Interface. The state can be one of the following: • Enabled: Indicates that the SIP Interface connected to the Realm is enabled. • Disabled: Indicates that the SIP Interface connected to the Realm is disabled.
RealmID	Indicates the name of the Realm to which the SIP Interface is associated.
In-manipulationid	Indicates the inbound SIP manipulation rule name.
Out-manipulationid	Indicates the outbound SIP manipulation rule name.
Options	Indicates the optional features and the parameters.
Last Modified By	Indicates the name of the user who last modified the configuration of the SIP Interface.
Last Modified Date	Indicates the date and time when the configuration of the SIP Interface was last modified.

SIP Ports

The **SIP Ports** tab lists the SIP ports of the SIP Interface. You can select a SIP port from the list displayed by the **SIP Ports** tab, and click to open the Acme SBC SIP Port Details form and view the details of the specific SIP port.

Network Interfaces

The **Network Interfaces** tab lists the Network Interfaces associated with the SIP Interface. You can select a Network Interface from the list displayed by the **Network Interfaces** tab, and click

to open the Acme SBC Network Interface Details form and view the details of the specific Network Interface.

Analysis Pane

The Analysis pane displays a summary of the details of the selected SIP Interface. For more information, see Monitoring SIP Interfaces.

Monitoring SIP Ports

The SIP Ports view on the right pane of the Acme SBC SIP Interface Details form displays the details of the SIP ports associated with a SIP Interface. The view arranges the key attributes of the SIP ports in a table.

To launch the SIP Ports view, follow this step:

- From the right pane of the Acme SBC SIP Interface Details form, select the **SIP Ports** tab. The SIP Ports view opens.

Basic Attributes of the SIP Ports Table

Attribute	Description
IP Address	Indicates the IP address of the SIP port.
Port	Indicates the port number used for the SIP port.
Transport Protocol	Indicates the transport protocol associated with the SIP port. The transport protocol can be one of the following: • TCP • UDP • TLS • SCTP

Acme SBC SIP Port Details Form

You can view the details of the selected SIP port using the Acme SBC SIP Port Details form.

To view the Acme SBC SIP Port Details form, follow this step:

- From the SIP Port view table, select the SIP port for which you want to view the details, and then click . The Acme SBC SIP Port Details form opens.

Filtering SIP Ports

You can filter the SIP ports, listed in the SIP Ports view, using the available filters. This feature enables you to view the SIP ports based on the filter option that you selected. You can perform the filtering action on all the columns available on the SIP ports view table.

Note: You can select multiple filters based on your requirements.

To filter the SIP Ports view, follow these steps:

1. Select a SIP port, listed in the SIP Ports view, and right-click one of the following column attributes:
   - **IP Address**
   - **Port**
   - **Transport Protocol**
2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the SIP ports that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the SIP ports for which the selected column is not empty.
   - **Is empty**: filters and lists all the SIP ports for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the SIP ports that do not have the value in the column that you selected.

The filtered list of the SIP ports appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected SIP ports on the Analysis pane. The following tabs and related details are displayed:

- **Acme SBC SIP Port Details Summary Tab**
  - IP Address: The IP address of the host associated with the SIP port.
  - Management Server: The management server for the selected SIP port. This attribute displays one of the following values:
    - **Local**: If the SIP port is being managed by the NNMi management server console on which you are viewing the SIP port details.
    - Name of the regional manager that manages the SIP port.

- **SIP Port Information Tab**
  - Port: Indicates the port number used for the SIP port.
  - Transport protocol: Indicates the transport protocol associated with the SIP port. The transport protocol can be one of the following:
    - TCP
    - UDP
    - TLS
    - SCTP
  - Allow Anonymous: Indicates the allow anonymous criteria for accepting and processing a SIP request from another SIP element. The available options are as follows:
    - All: all requests from any SIP elements are allowed.
    - Agents-only: only requests from configured session agents are allowed.
    - Realm-prefix: the source IP address of the request must fall within the realm address-prefix or a SIP interface sub-realm.
    - Registered: only requests from user agents that have an entry in the registration cache are allowed; with the exception of a REGISTER request. A REGISTER request is allowed from any user agent.
    - Register-prefix: a REGISTER request is allowed only when the source IP address of the request falls within the realm address-prefix or a SIP interface sub-realm.

SIP Port Details Form

The SIP Port Details form displays the general attributes of the SIP port.

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
IP Address	Indicates the IP address of the host associated with the SIP port.
Port	Indicates the port number used for the SIP port.

Attribute	Description
Transport Protocol	Indicates the transport protocol associated with the SIP port. The transport protocol can be one of the following: • TCP • UDP • TLS • SCTP
Allow-anonymous	Allow Anonymous: Indicates the allow anonymous criteria for accepting and processing a SIP request from another SIP element. The available options are as follows: • All: all requests from any SIP elements are allowed. • Agents-only: only requests from configured session agents are allowed. • Realm-prefix: the source IP address of the request must fall within the realm address-prefix or a SIP interface sub-realm. • Registered: only requests from user agents that have an entry in the registration cache are allowed; with the exception of a REGISTER request. A REGISTER request is allowed from any user agent. • Register-prefix: a REGISTER request is allowed only when the source IP address of the request falls within the Realm address-prefix or a SIP interface sub-realm.

Analysis Pane

The Analysis pane displays a summary of the details of the selected SIP port. For more information, see Monitoring SIP Ports.

Monitoring Session Agent Statistics

The Session Agent Statistics view displays the details of the Session Agents associated with a Session Director. The view arranges the key attributes of the Session Agents in a table.

To launch the Session Agent Statistics view, follow these steps:

1. From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Acme Session Director view opens on the right pane.
2. Select the Session Director for which you want to launch the Session Agent Statistics view, and then click . The Session Director Details form opens.

3. On the right pane of the form, click the **Session Agent Statistics** tab. The Session Agent Statistics view opens.

Basic Attributes of the Session Agent Statistics Table

Attribute	Description
Status	Indicates the current status of the Session Agent. The status can be one of the following: • Disabled • OutOfService • Standby • InService • ConstraintsViolation • InServiceTimedOut • OosProvisionedResponse • Unknown
Host Name	Indicates the host name of the Session Agent.
IP Address	Indicates the IP address of the Session Agent.

Session Agent Statistics Details Form

You can view the details of the selected Session Agent using the Session Agent Statistics Details form.

To view the Session Agent Statistics Details form, follow this step:

- From the Session Agent Statistics view table, select the Session Agent for which you want to view the details, and then click . The Session Agent Statistics Details form opens.

Filtering Session Agent Statistics

You can filter the Session Agents, listed in the Session Agent Statistics view, using the available filters. This feature enables you to view the Session Agent Statistics based on the filter option that you selected. You can perform the filtering action on all the columns available on the Session Agent Statistics view table.

Note: You can select multiple filters based on your requirements.

To filter the Session Agent Statistics view, follow these steps:

1. Select a Session Agent, listed in the Session Agent Statistics view, and right-click one of the following column attributes:
   - **Status**
   - **Host Name**
   - **IP Address**
2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the Session Agents that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the Session Agents for which the selected column is not empty.
   - **Is empty**: filters and lists all the Session Agents for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the Session Agents that do not have the value in the column that you selected.

The filtered list of the Session Agent Statistics appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected Session Agent on the Analysis pane. The following tabs and related details are displayed:

- **Session Agent Statistics Details Summary Tab**
  - Host Name: The host name of the Session Agent.
  - IP Address: The IP address of the Session Agent.
  - Tenant: The name of the tenant to which the Session Agent belongs.
  - Management Server: The management server for the selected Session Agent. This attribute displays one of the following values:
    - **Local**: If the Session Agent is being managed by the NNMi management server console on which you are viewing the Session Agent details.
    - Name of the regional manager that manages the Session Agent.
- **Session Agent Statistics Information Tab**

- State:Indicates the state of the Session Agent. The state can be one of the following:
  - Enabled - indicates that the Session Agent is enabled.
  - Disabled - indicates that the Session Agent is disabled.
- App-protocol: The protocol on which message is sent to the Session Agent.
- Realm-id: The ID of the Realm for session coming from or going to the Session Agent.
- Description: A brief description of the Realm in which the Session Agent resides.
- Last-modified-by: The name of the user who last modified the configuration of the Session Agent.
- Last-modified-date: The date and time when the configuration of the Session Agent was last modified.

Session Agent Statistics Details Form

The Session Agent Statistics Details form is split into two panes. The left pane displays the general attributes of the Session Agent. The right pane (**Realms** tab) displays the list of realms associated with the Session Agent. For more information about **Realms** tab, see Monitoring Realms.

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
Host Name	Indicates the host name of the Session Agent.
IP Address	Indicates the IP address of the Session Agent.

Attribute	Description
Status	Indicates the current status of the Session Agent. The status can be one of the following: • Disabled • OutOfService • Standby • InService • ConstraintsViolation • InServiceTimedOut • OosProvisionedResponse • Unknown
transport-method	Indicates the IP protocol used to communicate with the Session Agent. The IP protocol can be one of the following: • UDP • UDP+TCP • DynamicTCP • StaticTCP
reuse-connections	Indicates the status of the "reuse-connections" feature of Acme Session Director. The status can be one of the following: • None: Indicates that the feature is turned off. • TCP: Indicates that the feature is enabled for TCP connections.

Analysis Pane

The Analysis pane displays a summary of the details of the selected Session Agent. For more information, see Monitoring Session Agent Statistics.

Monitoring Session Agent Groups

The Session Agent Group view displays the details of the Session Agent Groups associated with a Session Director. The view arranges the key attributes of the Session Agent Groups in a table.

To launch the Session Agent Group view, follow these steps:

1. From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Acme Session Director view opens on the right pane.
2. Select the Session Director for which you want to launch the Session Agent Group view, and then click . The Session Director Details form opens.
3. On the right pane of the form, click the **Session Agent Group** tab. The Session Agent Group view opens.

Basic Attributes of the Session Agent Group Table

Attribute	Description
State	The state of the Session Agent Group on the Session Director. The state can be one of the following: • Enabled: Indicates that the Session Agent Group on the Session Director is enabled. • Disabled: Indicates that the Session Agent Group on the Session Director is disabled.
Group Name	Indicates the unique name of the Session Agent Group.
Application Protocol	Indicates the signaling protocol used with the Session Agent Group. The valid values are as follows: • SIP • H323
Strategy	Indicates the Session Agent allocation strategy to select the Session Agents to be made available by the Session Agent Group. The available values are: • Hunt: Selects Session Agents in the order which they are listed. • RoundRobin: Selects each Session Agent in the order in which it is listed in the destination list. • LeastBusy: Selects the Session Agent that has the fewest number of sessions relative to the maximum outbound sessions constraint or the maximum sessions constraint. • PropDist: Indicates the Proportional Distribution strategy. It proportionally distributes the traffic among all the available session agents. • LowSusRate: Indicates Low Sustained Rate. It routes to the Session Agent with the lowest sustained rate of session initiations/invitations.
Description	A brief description of the Session Agent Group.

Session Agent Group Details Form

You can view the details of the selected Session Agent Group using the Acme SBC Session Agent Group Details form.

To view the Acme SBC Session Agent Group Details form, follow this step:

- From the Session Agent Group view table, select the Session Agent Group for which you want to view the details, and then click . The Acme SBC Session Agent Group Details form opens.

Filtering Session Agent Groups

You can filter the Session Agent Groups, listed in the Session Agent Group view, using the available filters. This feature enables you to view the Session Agent Groups based on the filter option that you selected. You can perform the filtering action on all the columns available on the Session Agent Group view table.

Note: You can select multiple filters based on your requirements.

To filter the Session Agent Group view, follow these steps:

1. Select a Session Agent Group, listed in the Session Agent Group view, and right-click one of the following column attributes:
   - **State**
   - **Group Name**
   - **Application Protocol**
   - **Strategy**
   - **Description**
2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the Session Agent Groups that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the Session Agent Groups for which the selected column is not empty.
   - **Is empty**: filters and lists all the Session Agent Groups for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the Session Agent Groups that do not have the value in the column that you selected.

The filtered list of the Session Agent Groups appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected Session Agent Group on the Analysis pane. The following tabs and related details are displayed:

- **Acme SBC Session Agent Group Details Summary Tab**
  - Group-name: The unique name of the Session Agent Group.
  - Description: A brief description of the Session Agent Group.
  - Tenant: The name of the tenant to which the Session Agent Group belongs.
  - Management Server: The management server for the selected Session Agent Group. This attribute displays one of the following values:
    - **Local**: If the Session Agent Group is being managed by the NNMi management server console on which you are viewing the Session Agent Group details.
    - Name of the regional manager that manages the Session Agent Group.
- **Session Agent Group Information Tab**
  - State:The state of the Session Agent Group on the Session Director. The state can be one of the following:
    - Enabled - indicates that the Session Agent Group is enabled.
    - Disabled - indicates that the Session Agent Group is disabled.
  - App-protocol: The signaling protocol used with the Session Agent Group.
  - Strategy: The Session Agent allocation strategy to select the Session Agents to be made available by the Session Agent Group.
  - Destination: The destinations (Session Agents) available for use by the Session Agent Group.
  - Sag-recursion: The state of the SIP Session Agent Group recursion parameter. The state can be one of the following:
    - Enabled
    - Disabled
  - Stop-sag-recurse: The list of SIP response codes that terminate recursion within the Session Agent Group.
  - Last-modified-by:

- Last-modified-date: The date and time when the monitoring of the Session Agent Group was last modified.

Session Agent Group Details Form

The Session Agent Group Details form is split into two panes. The left pane displays the general attributes of the session agent. The right pane displays the following tabs:

- Session Agents- displays the list of Session Agents associated with the Session Agent Group.For more information about **Session Agents**tab, see Monitoring Session Agents.
- Realms - displays the list of realms associated with the Session Agent Group.For more information about **Realms** tab, see Monitoring Realms.

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
Group Name	Indicates the unique name of the Session Agent Group.
Description	A brief description of the Session Agent Group.
State	The state of the Session Agent Group on the session director. The state can be one of the following: • Enabled: Indicates that the Session Agent Group on the Session Director is enabled. • Disabled: Indicates that the Session Agent Group on the Session Director is disabled.
Application Protocol	Indicates the signaling protocol used with the Session Agent Group.The valid values are as follows: • SIP • H323

Attribute	Description
Strategy	Indicates the session agent allocation strategy to select the Session Agents to be made available by the Session Agent Group.The available values are: • Hunt: Selects Session Agents in the order which they are listed. • RoundRobin: Selects each session agent in the order in which it is listed in the destination list. • LeastBusy: Selects the session agent that has the fewest number of sessions relative to the maximum outbound sessions constraint or the maximum sessions constraint. • PropDist: Indicates the Proportional Distribution strategy. It proportionally distributes the traffic among all the available session agents. • LowSusRate: Indicates Low Sustained Rate. It routes to the session agent with the lowest sustained rate of session initiations/invitations.
Trunk-group	Indicates the trunk group names and trunk group contexts associated with the session agent group.
Sag-recursion	Indicates the state of the SIP Session Agent Group recursion parameter. The state can be one of the following: • Enabled • Disabled
Stop-sag-recurse	Indicates the list of SIP response codes that terminate recursion within the Session Agent Group.
Last-modified-by	Indicates the name of the user who last modified the configuration of the session agent group.
Last-modified-date	Indicates the date and time when the configuration of the Session Agent Group was last modified.

Analysis Pane

The Analysis pane displays a summary of the details of the selected Session Agent Group. For more information, see Monitoring Session Agent Groups.

Monitoring Network Interfaces

The Network Interface view displays the details of the Acme SBC Network Interfaces associated with a Session Director or a Realm. The view arranges the key attributes of the Network Interfaces in a table.

To launch the Network Interface view, follow these steps:

1. From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Acme Session Director view opens on the right pane.
2. Select the Session Director for which you want to launch the Network Interface view, and then click . The Session Director Details form opens.
3. On the right pane of the form, click the **Network Interface** tab. The Network Interface view opens.

Basic Attributes of the Network Interface Table

Attribute	Description
Name	Indicates the name of the Acme SBC Network Interface.
Sub-port	Indicates the sub-port ID.
IP Address	Indicates the IP address of the Network Interface.
Description	A brief description of the Network Interface.

Network Interface Details Form

You can view the details of the selected session agent using the Acme SBC Network Interface Details form.

To view the Acme SBC Network Interface Details form, follow this step:

- From the Network Interface view table, select the Network Interface for which you want to view the details, and then click . The Acme SBC Network Interface Details form opens.

Filtering Network Interfaces

You can filter the Network Interfaces, listed in the Network Interface view, using the available filters. This feature enables you to view the Network Interfaces based on the filter option that you selected. You can perform the filtering action on all the columns available on the Network Interface view table.

Note: You can select multiple filters based on your requirements.

To filter the Network Interface view, follow these steps:

1. Select a Network Interface, listed in the Network Interface view, and right-click one of the following column attributes:
   - **Name**
   - **Sub-port**

- **IP Address**
- **Description**

2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the Network Interfaces that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the Network Interfaces for which the selected column is not empty.
   - **Is empty**: filters and lists all the Network Interfaces for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the Network Interfaces that do not have the value in the column that you selected.

The filtered list of the Network Interfaces appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected Network Interface on the Analysis pane. The following tabs and related details are displayed:

- **Acme SBC Network Interface Details Summary Tab**
  - Name: The name of the Network Interface.
  - Sub-port-id: The sub port ID of the Network Interface.
  - Tenant: The name of the tenant to which the Network Interface belongs.
  - Management Server: The management server for the selected Network Interface. This attribute displays one of the following values:
    - **Local**: If the Network Interface is being managed by the NNMi management server console on which you are viewing the Network Interface details.
    - Name of the regional manager that manages the Network Interface.
- **Network Interface Information Tab**
  - IP Address: The IP address of the Network Interface.

- Description: A brief description of the Network Interface.
- Pri-utility-addr: The utility IP address of the primary HA peer in an HA architecture.
- Sec-utility-addr: The utility IP address of the secondary Acme SBC peer in an HA architecture.
- Netmask: The destination subnet mask of the Network Interface.
- Gateway: The gateway that this Network Interface uses to forward packets.
- Hip-ip-list: The list of Host Identity Protocol IP addresses associated with the Network Interface.
- Icmp-address: The ICMP address associated with the Network Interface.

- **Realm Statistics Tab**
  - Inbound Current Active Sessions: Number of active inbound sessions for the Realm.
  - Inbound Current Session Rate: Call per second (CPS) rate of active inbound sessions for the Realm.
  - Outbound Current Active Sessions: Number of active outbound sessions for the Realm.
  - Outbound Current Session Rate: CPS rate of active outbound sessions for the Realm.
  - Inbound Total Sessions: Total number of inbound sessions for the Realm.
  - Outbound Total Sessions: Total number of outbound sessions for the Realm.

Network Interface Details Form

The Network Interface Details form is split into two panes. The left pane displays the following details:

- **General**
- **Gateway Heart Beat**

The right pane displays the following tabs:

- Realms - displays the list of Realms associated with the Network Interface. For more information about **Realms** tab, see Monitoring Realms.
- SIP Interfaces - displays the list of SIP interfaces associated with the Network Interface. For more information about **SIP Interfaces** tab, see Monitoring SIP Interfaces.

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
Name	Indicates the name of the Acme SBC Network Interface.
Sub-port	Indicates the sub-port ID.
IP Address	Indicates the IPv4 address of the Network Interface.
Description	A brief description of the Network Interface.
Pri-utility-addr	Indicates the utility IP address of the primary HA peer in an HA architecture.
Sec-utility-addr	Indicates the utility IP address of the secondary Acme SBC peer in an HA architecture.
Netmask	Indicates the destination subnet mask of the Network Interface.
Gateway	Indicates the gateway that this Network Interface uses to forward packets.
Hip-ip-list	Indicates the list of Host Identity Protocol IP addresses associated with the Network Interface.
Icmp-Address	Indicates the ICMP address associated with the Network Interface.

Gateway Heart Beat

The attributes that appear under the **Gateway Heart Beat** section are described in the following table:

Attribute	Description
State	Indicates the state of the front interface link detection and polling functionality on the Acme SBC for the network-interface element. The state can be one of the following: • Enabled • Disabled
Heartbeat	Indicates the time interval in seconds between heartbeats for the front interface gateway.
Retry-count	Indicates the number of front interface gateway heartbeat retries before a gateway is considered unreachable.
Health-score	Indicates the amount to subtract from the health score if the front interface gateway heartbeat fails.

Analysis Pane

The Analysis pane displays a summary of the details of the selected Network Interface. For more information, see Monitoring Network Interfaces.

Viewing Discovered Acme Licenses

The License view displays the details of the licenses associated with a Session Director. The view arranges the key attributes of the licenses in a table.

To launch the License view, follow these steps:

1. From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Acme Session Director view opens on the right pane.
2. Select the Session Director for which you want to launch the License view, and then click . The Session Director Details form opens.
3. On the right pane of the form, click the **License** tab. The License view opens.

Basic Attributes of the License Table

Attribute	Description
License Key	Indicates the license key of the Session Director.
Capacity	Indicates the maximum number of simultaneous sessions allowed by the Session Director for all combined protocols.
Expire Date	Indicates the end date of the license.
Install Date	Indicates the date of install of license on the Session Director.
Begin Date	Indicates the start date of the license.
Protocol Names	Indicates the licensed protocols. The possible values are: • SIP • MGCP • H323

License Details Form

You can view the details of the selected license using the Acme SBC License Details form.

To view the Acme SBC License Details form, follow this step:

- From the License view table, select the license for which you want to view the details, and then click . The Acme SBC License Details form opens.

Filtering Licenses

You can filter the licenses, listed in the License view, using the available filters. This feature enables you to view the licenses based on the filter option that you selected. You can perform the filtering action on all the columns available on the License view table.

Note: You can select multiple filters based on your requirements.

To filter the License view, follow these steps:

1. Select a license, listed in the License view, and right-click one of the following column attributes:
   - **License Key**
   - **Capacity**
   - **Expire Date**
   - **Install Date**
   - **Begin Date**
   - **Protocol Names**
2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the licenses that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the licenses for which the selected column is not empty.
   - **Is empty**: filters and lists all the licenses for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the licenses that do not have the value in the column that you selected.

The filtered list of the licenses appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected license on the Analysis pane. The following tabs and related details are displayed:

- **Acme SBC License Details Summary Tab**
  - License Key: The license key of the Session Director.
  - Capacity: The maximum number of simultaneous sessions allowed by the Session Director for all combined protocols.
  - Install Date: The date of install of license on the Session Director.
  - Begin Date: The start date of the license.
  - Expire Date: The end date of the license.
  - Protocol Names: The licensed protocols. The possible values are:
    - SIP
    - MGCP
    - H323
  - Enabled Feature Names: The licensed features. For example, Interworking Feature (IWF), Quality of Service (QoS)

License Details Form

The License Details form displays the general attributes of the license associated with the Session Director.

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
License Key	Indicates the license key of the Session Director.
Capacity	Indicates the maximum number of simultaneous sessions allowed by the Session Director for all combined protocols.
Install Date	Indicates the date of install of the Session Director.
Begin Date	Indicates the start date of the license.
Expire Date	Indicates the end date of the license.

Attribute	Description
Protocol Names	Indicates the licensed protocols. The possible values are: • SIP • MGCP • H323
Enabled Feature Names	Indicates the licensed features. For example, Interworking Feature (IWF), Quality of Service (QoS)

Analysis Pane

The Analysis pane displays a summary of the details of the selected license. For more information, see Viewing Discovered Acme SBC Licenses.

Viewing Discovered Acme Software

The Software view displays the details of the Acme software discovered by the NNM iSPI for IP Telephony. The view arranges the key attributes of the software in a table.

To launch the Software view, follow these steps:

1. From the **Workspaces** navigation pane, click **Acme IP Telephony** > **Session Director**. The Acme Session Director view opens on the right pane.
2. Select the Session Director for which you want to launch the Software view, and then click . The Session Director Details form opens.
3. On the right pane of the form, click the **Software** tab. The Software view opens.

Basic Attributes of the Software Table

Attribute	Description
Status	Indicates if the software is used currently or was in use previously.
Type	Indicates the type of software.
Description	A brief description of the Acme SBC software.

Software Details Form

You can view the details of the selected software using the Acme SBC Software Details form.

To view the Acme SBC Software Details form, follow this step:

- From the Software view table, select the Software for which you want to view the details, and then click . The Acme SBC Software Details form opens.

Filtering Software

You can filter the software, listed in the Software view, using the available filters. This feature enables you to view the software based on the filter option that you selected. You can perform the filtering action on all the columns available on the Software view table.

Note: You can select multiple filters based on your requirements.

To filter the Software view, follow these steps:

1. Select a software, listed in the Software view, and right-click one of the following column attributes:
   - **Description**
   - **Type**
   - **Status**
2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the software that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the software for which the selected column is not empty.
   - **Is empty**: filters and lists all the software for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the software that do not have the value in the column that you selected.

The filtered list of the software appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected software on the Analysis pane. The following tabs and related details are displayed:

- **Acme SBC Software Details Summary Tab**
  - Description: A brief description of the Acme SBC software.
  - Type: The type of software.
  - Status: If the software is used currently or was in use previously.

Acme SBC Software Details Form

The Acme SBC Software Details form displays the general attributes of the Acme SBC software discovered and monitored by the NNM iSPI for IP Telephony.

General

The attributes that appear under the **General** section are described in the following table:

Basic Attributes of the Software Table

Attribute	Description
Description	A brief description of the Acme SBC software.
Type	Indicates the type of software.
Status	Indicates if the software is used currently or was in use previously.

Analysis Pane

The Analysis pane displays a summary of the details of the selected software. For more information, see Viewing Discovered Acme SBC Software.

Monitoring Configuration for Acme Session Director

The Monitoring Configuration feature enables you to monitor the following:

- Performance data on a per-realm basis. You can use this data to configure the monitoring of discovered Session Directors, Realms, and Network Interfaces.
- Management of the System. You can use this data to configure the monitoring of the percentage of licensed sessions that are in progress for a Session Director, the calls per second, and the concurrent sessions of the system.
- Session Initiation Protocol (SIP) sessions statistics
- SIP errors. You can use this data to configure the monitoring of the errors that occur in SIP media events.
- SIP Access Control List (ACL) operations statistics
- SIP transactions statistics
- SIP client states statistics
- SIP server states statistics
- SIP invites statistics
- Session Agent statistics

This feature also helps you to configure settings such as enabling reporting, and specifying threshold settings for generating incidents.

To open the Monitoring Configuration for Acme SBC window, follow this step:

- From the **Session Director** inventory, select a discovered device, and then click **Actions > IP Telephony > Monitoring Configuration**.

In the Monitoring Configuration window, you can select additional monitoring attributes of the selected device. After configuration, you can view the states of these additional attributes in the following formats:

- Analysis pane in the Session Director inventories

> **Note:** You can view the Realm Statistics in the Realm and Network Interface inventories also.

- Reports
- Performance Graphs
- *If you configure thresholds.* Incidents in the incidents inventory

> **Note:** You can perform monitoring configuration only on a locally discovered node.

> **Note:** You cannot open multiple Monitoring Configuration windows at the same time. Before opening a new Monitoring Configuration window, make sure to click (the **Save** icon) in the existing Monitoring Configuration window to prevent loss of configuration data.

Monitoring with Performance Graphs

Based on the Monitoring Configurations that are enabled for a Session Director, you can view real-time performance data for the Session Director with the help of performance graphs. The NNM iSPI for IP Telephony collects the performance data from the Network Performance Server (NPS) to display intuitive graphs of the data in the troubleshooting workbench (NNM iSPI for IP Telephony Performance Graphing window). This feature gives you the options to view the following:

- Graphs with predefined metrics
- Graphs with the selected metric class and the related metrics

Prerequisites for Viewing the Acme IP Telephony Performance Graphs

Make sure that the following prerequisites are satisfied to enable the viewing of the performance graphs of Acme IP Telephony:

1. Install the NNM iSPI Performance for Metrics (iSPI Performance for Metrics) in your deployment environment before installing the NNM iSPI for IP Telephony.
2. Enable the various monitoring configurations for Acme IP Telephony.
3. Verify that the iSPI Performance for Metrics is running so that the NNM iSPI for IP Telephony can collect the performance data from NPS.

The performance graphs for the Session Directors are launched externally using a URL action from the Acme IP Telephony inventory.

To launch the graphs, follow this step:

- From the **Session Director** inventory, select a discovered device, and then click **Actions > IP Telephony Reports > Performance Graphs**. The external troubleshooting workbench (NNM iSPI for IP Telephony Performance Graphing window) opens.

The components of the troubleshooting workbench are described in the following table:

Components	Description
Configuration Items pane	Displays the name of the selected discovered device.
Predefined Graphs tab	Displays the graphs with predefined metrics for the selected discovered device.
Metrics tab	Allows you to select metric classes and related metrics to view the graph on the right panel. To view the graphs using the **Metrics** tab, follow these steps: 1. From the **Metric Classes** section, select a measure. For example, System Management For Acme SBC. The **Metrics** section now displays the measurement attributes for the selected measure. 2. From the **Metrics** section, select the attribute for which you want to view the graph, and then drag and drop it into the right panel. The right panel displays the performance graph for the selected metrics.
Right Panel	Displays the predefined graphs and the ones based on the selected metrics.

Monitoring Realm Statistics

You can configure the NNM iSPI for IP Telephony to monitor the Realm Statistics at the Realm, Network Interface and Session Director levels. The following table lists the details of the types of measurement attributes that you can configure for monitoring Realm Statistics:

Realm Statistics	Description

Inbound Current Active Sessions	Indicates the number of active inbound sessions for the realm.
Inbound Current Session Rate	Indicates the CPS rate of active inbound sessions for the realm.
Outbound Current Active Sessions	Indicates the number of active outbound sessions for the realm.
Outbound Current Session Rate	Indicates the CPS rate of active outbound sessions for the realm.
Inbound Total Sessions	Indicates the total number of inbound sessions for the realm.
Outbound Total Sessions	Indicates the total number of outbound sessions for the realm.

Enabling the Monitoring of Realm Statistics

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of Realm Statistics. The page displays the list of existing Realm Statistics configuration settings under the **Realm Statistics** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of Realm Statistics, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.
3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click a device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.
4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **Realm Statistics** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring Realm Statistics Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the Realm Statistics setting, go to **Step 5**.
7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the Realm Statistics for the Session Director. The

default value is five minutes. You can select only a value that is greater than the default value.

8. Click (the **Save** icon) to save the monitoring configuration.

The measurements added at the Session Director level result in the addition of these measurements at the Realm and Network Interface level also. You can select a Realm or a Network Interface from the Session Director Details form and click **Actions** > **IP Telephony** > **Monitoring Configuration** from the menu to launch the **Monitoring Configuration for Acme SBC** page for the selected Realm or Network Interface. At the Realm and Network Interface level, this page enables you to modify a threshold setting to generate incidents for a selected Realm or Network Interface. However, you cannot specify the data collection intervals here. You must always specify them at the Acme Session Director level. Individual Realms and Network Interfaces assume the intervals specified for the corresponding Session Director.

Note: You cannot add a new measurement type at the Realm and Network Interface levels. However, you can add the measurement types, which are already added at the Session Director level, to the Realms or Network Interfaces discovered after the addition of these measurement types.

To modify an existing Realm Statistics configuration setting, follow these steps:

1. Select the Realm Statistics configuration that you want to modify and click **Edit**. The **Add/Update Acme Realm Statistics** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing Realm Statistics configuration setting, follow this step:

- Select the Realm Statistics configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing Realm Statistics configuration settings.

To disable an existing Realm Statistics configuration setting, follow this step:

- Select the Realm Statistics configuration that you want to disable, and then click **Disable All**.

Note: The **Delete**, **Delete All**, and **Disable All** buttons are enabled only at the **Acme Session Director** level.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the regional managers.

Configuring the Realm Statistics Settings

The **Add/Update Acme Realm Statistics** page enables you to define the attributes for configuring Realm Statistics.

To configure Realm Statistics settings, follow these steps:

1. On the **Add/Update Acme Realm Statistics** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the Realm Statistics type that is to be monitored. You can select one of the following types: ▪ **Inbound Current Active Sessions** ▪ **Inbound Current Session Rate** ▪ **Outbound Current Active Sessions** ▪ **Outbound Current Session Rate** ▪ **Inbound Total Sessions** ▪ **Outbound Total Sessions** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the Realm Statistics type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the Realm Statistics type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Monitoring System Management Statistics

You can configure the NNM iSPI for IP Telephony to monitor the System Management Statistics of a Session Director in use. The following table lists the details of the types of measurement

attributes that you can configure for monitoring System Management Statistics:

System Management Statistics	Description
License Capacity	Indicates the percentage of the licensed Session Directors in use.
Calls Per Second	Indicates the instant number (gauge value) of the calls per second (signaling rate) on the system.
Concurrent Sessions	Indicates the instant number (gauge value) of the total concurrent signaling sessions on the system.

Enabling the Monitoring of System Management Statistics

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the percentage of licensed sessions of a Session Director. The page displays the System Management Statistics configuration settings for the selected Session Director, under the **System** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of System Management Statistics, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.
3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click a device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.
4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **System** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding Measurement Type, see Configuring System Management Statistics Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the System Management Statistics setting, go to **Step 5**.
7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the percentage of the licensed sessions for the Session Director. The default value is five minutes. You can select only a value that is greater than the default value.
8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing System Management Statistics configuration setting, follow these steps:

1. Select the System Management Statistics configuration that you want to modify and click **Edit**. The **Add/Update Acme System Management Statistics** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing System Management Statistics configuration setting, follow this step:

- Select the System Management Statistics configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing System Management Statistics configuration settings.

To disable an existing System Management Statistics configuration setting, follow this step:

- Select the System Management Statistics configuration that you want to disable, and then click **Disable All**.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the regional managers.

Configuring the System Management Statistics Settings

The **Add/Update Acme System Management Statistics** page enables you to define the attributes for configuring System Management Statistics.

To configure System Management Statistics, follow these steps:

1. On the **Add/Update Acme System Management Statistics** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the measurement type that is to be monitored. You can select one of the following types: ▪ **License capacity** ▪ **Calls per second** ▪ **Concurrent sessions** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.

Lower Base	Specify the lower base value for the System Management Statistics type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the System Management Statistics type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Monitoring SIP Sessions

You can configure the NNM iSPI for IP Telephony to monitor the Session Initiation Protocol (SIP) sessions statistics. The following table lists the details of the types of measurement attributes that you can configure for monitoring SIP sessions statistics:

SIP Sessions Statistics	Description
Sessions	Indicates the total number of sessions established by the **Invite** and **Subscribe** messages.
Sessions Initial	Indicates the total number of sessions for which an **Invite** or **Subscribe** is being forwarded.
Sessions Early	Indicates the total number of sessions for which the first provisional response is received.
Sessions Established	Indicates the total number of sessions for which a success response is received.

Sessions Terminated	Indicates the total number of sessions that have ended by receiving or sending a **Bye** for an **Established** session or forwarding an error response for an **Initial** or **Early** session. The session remains in the terminated state until all the resources for the session are free.
Dialogs	Indicates the total number of end-to-end SIP signaling connections.
Dialogs Early	Indicates the total number of dialogs that were created by a provisional response.
Dialogs Confirmed	Indicates the total number of dialogs that were created by a success response. **Note:** An **Early** dialog becomes **Confirmed** when a success response is received.
Dialogs Terminated	Indicates the total number of dialogs that have ended by receiving or sending a **Bye** for an **Established** dialog or forwarding an error response for an **Initial** or **Early** dialog. The dialog remains in the terminated state until all the resources for the session are free.

Enabling the Monitoring of SIP Sessions

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the SIP sessions of a Session Director. The page displays the SIP Sessions configuration settings for the selected Session Director, under the **SIP Sessions** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of SIP Sessions, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.
3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click an active device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.
4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **SIP Sessions** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding Measurement Type, see Configuring the SIP Sessions Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the SIP Sessions setting, go to **Step 5**.

7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the SIP sessions of the Session Director. The default value is five minutes. You can select only a value that is greater than the default value.

8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing SIP Sessions configuration setting, follow these steps:

1. Select the SIP Sessions configuration that you want to modify and click **Edit**. The **Add/Update Acme SIP Sessions** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing SIP Sessions configuration setting, follow this step:

- Select the SIP Sessions configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing SIP Sessions configuration settings.

To disable an existing SIP Sessions configuration setting, follow this step:

- Select the SIP Sessions configuration that you want to disable, and then click **Disable All**.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the Regional Managers.

Configuring the SIP Sessions Settings

The **Add/Update Acme SIP Sessions** page enables you to define the attributes for configuring SIP Sessions.

To configure SIP Sessions, follow these steps:

1. On the **Add/Update Acme SIP Sessions** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the measurement type that is to be monitored. You can select one of the following types: ▪ **Sessions** ▪ **Sessions Initial** ▪ **Sessions Early** ▪ **Sessions Established** ▪ **Sessions Terminated** ▪ **Dialogs** ▪ **Dialogs Early** ▪ **Dialogs Confirmed** ▪ **Dialogs Terminated** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the SIP Sessions type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the SIP Sessions type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Note: Make sure to add the configuration settings manually to the redundant standby pair of the active Session Director.

Monitoring SIP Errors

You can configure the NNM iSPI for IP Telephony to monitor the statistics of the errors that occur in SIP media events. The following table lists the details of the types of measurement attributes that you can configure for monitoring SIP sessions statistics:

SIP Errors Statistics	Description
SDP Offer Errors	Indicates the total number of errors encountered in setting up the media session for a session description in a SIP request/response of a Session Description Protocol (SDP) Offer.
SDP Answer Errors	Indicates the total number of errors encountered in setting up the media session for a session description in a SIP request/response of a Session Description Protocol (SDP) Answer.
Drop Media Errors	Indicates the total number of errors encountered in tearing down the media for a dialog or session that is terminated due to one of the following reasons: • Unsuccessful response to an INVITE transaction • A BYE transaction received from one of the participants in a dialog/session • A BYE initiated by the Session Director due to a timeout notification from the Middlebox Control Daemon (MBCD).
Transaction Errors	Indicates the total number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session.
Application Errors	Indicates the total number of miscellaneous errors in the SIP application that are otherwise not categorized.
Call Rejects	Indicates the total number of rejected calls.
Media Exp Events	Indicates the total number of flow timer expiration notifications received from the MBCD.
Early Media Exps	Indicates the total number of flow timer expiration notifications received for media sessions that were not completely set up due to an incomplete or pending INVITE transaction.
Exp Media Drops	Indicates the total number of flow timer expiration notifications from the MBCD that resulted in the termination of the dialog/session by the SIP application.
Expired Sessions	Indicates the total number of sessions terminated due to the session timer expiring.

Multiple OK Drops	Indicates the total number of dialogs terminated upon reception of a 200 OK response from multiple User Agent Servers (UASs) for a given INVITE transaction that was forked by a downstream proxy.
Multiple OK Terms	Indicates the total number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the Session Director.
Media Failure Drops	Indicates the total number of dialogs terminated due to a failure in establishing the media session.
Non-ACK 2xx Drops	Indicates the total number of sessions terminated because an ACK was not received for a 2xx response.
Invalid Requests	Indicates the total number of invalid requests.
Invalid Responses	Indicates the total number of invalid responses.
Invalid Messages	Indicates the total number of messages dropped due to parse failure.
CAC Session Drop	Indicates the total number of Call Admission Control (CAC) session setup failures.
CAC BW Drop	Indicates the total number of CAC session setup failures due to insufficient BW (bandwidth).

Enabling the Monitoring of SIP Errors

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the errors that occur in a SIP media events of a Session Director. The page displays the SIP Errors configuration settings for the selected Session Director, under the **SIP Errors** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of SIP Errors, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.
3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click an active device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.

4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **SIP Errors** from the **Area of Monitoring** drop-down list.

5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding Measurement Type, see Configuring the SIP Errors Settings.

6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the SIP Errors setting, go to **Step 5**.

7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the errors that occur in the SIP media events of the Session Director. The default value is five minutes. You can select only a value that is greater than the default value.

8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing SIP Errors configuration setting, follow these steps:

1. Select the SIP Errors configuration that you want to modify and click **Edit**. The **Add/Update Acme SIP Errors** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing SIP Errors configuration setting, follow this step:

- Select the SIP Errors configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing SIP Errors configuration settings.

To disable an existing SIP Errors configuration setting, follow this step:

- Select the SIP Errors configuration that you want to disable, and then click **Disable All**.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the Regional Managers.

Configuring the SIP Errors Settings

The **Add/Update Acme SIP Errors** page enables you to define the attributes for configuring the settings for the errors that occur in the SIP media events.

To configure SIP Errors, follow these steps:

1. On the **Add/Update Acme SIP Errors** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the measurement type that is to be monitored. You can select one of the following types: ▪ **SDP Offer Errors** ▪ **SDP Answer Errors** ▪ **Drop Media Errors** ▪ **Transaction Errors** ▪ **Application Errors** ▪ **Call Rejects** ▪ **Media Exp Events** ▪ **Early Media Exps** ▪ **Exp Media Drops** ▪ **Expired Sessions** ▪ **Multiple OK Drops** ▪ **Multiple OK Terms** ▪ **Media Failure Drops** ▪ **Non-ACK 2xx Drops** ▪ **Invalid Requests** ▪ **Invalid Responses** ▪ **Invalid Messages** ▪ **CAC Session Drop** ▪ **CAC BW Drop** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.

Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the SIP Errors type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the SIP Errors type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.

Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Note: Make sure to add the configuration settings manually to the redundant standby pair of the active Session Director.

Monitoring SIP ACL Operations

You can configure the NNM iSPI for IP Telephony to monitor the statistics of SIP ACL operations. The following table lists the details of the types of measurement attributes that you can configure for monitoring SIP ACL operations statistics:

SIP Sessions Statistics	Description
ACL Requests	Indicates the total number of ACL requests.
Bad Messages	Indicates the total number of bad messages.
Promotions	Indicates the total number of ACL entry promotions.
Demotions	Indicates the total number of ACL entry demotions.
Demote Trust-Untrust	Indicates the total number of ACL entries demoted from trusted to untrusted.
Demote Untrust-Deny	Indicates the total number of ACL entries demoted from untrusted to deny.

Enabling the Monitoring of SIP ACL Operations

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the SIP ACL operations of a Session Director. The page displays the SIP ACL operations configuration settings for the selected Session Director, under the **SIP ACL Operations** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of SIP ACL operations, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.

3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click an active device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.

4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **SIP ACL Operations** from the **Area of Monitoring** drop-down list.

5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding Measurement Type, see Configuring the SIP ACL Operations Settings.

6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the SIP ACL Operations setting, go to **Step 5**.

7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the SIP ACL operations of the Session Director. The default value is five minutes. You can select only a value that is greater than the default value.

8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing SIP ACL operations configuration setting, follow these steps:

1. Select the SIP ACL operations configuration that you want to modify and click **Edit**. The **Add/Update Acme SIP ACL Operations** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing SIP ACL operations configuration setting, follow this step:

- Select the SIP ACL operations configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing SIP ACL operations configuration settings.

To disable an existing SIP ACL operations configuration setting, follow this step:

- Select the SIP ACL operations configuration that you want to disable, and then click **Disable All**.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the Regional Managers.

Configuring the SIP ACL Operations Settings

The **Add/Update Acme SIP ACL Operations** page enables you to define the attributes for configuring the SIP ACL operations settings.

To configure SIP ACL operations, follow these steps:

1. On the **Add/Update Acme SIP ACL Operations** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the measurement type that is to be monitored. You can select one of the following types: ▪ **ACL Requests** ▪ **Bad Messages** ▪ **Promotions** ▪ **Demotions** ▪ **Demote Trust-Untrust** ▪ **Demote Untrust-Deny** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the SIP ACL Operations type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the SIP ACL Operations type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Note: Make sure to add the configuration settings manually to the redundant standby pair of the active Session Director.

Monitoring SIP Transactions

You can configure the NNM iSPI for IP Telephony to monitor the statistics of SIP transactions. The following table lists the details of the types of measurement attributes that you can configure for monitoring the statistics of SIP transactions:

SIP Transactions Statistics	Description
Sessions	Indicates the total number of sessions established by INVITE and SUBSCRIBE messages.
Subscriptions	Indicates the total number of sessions established by SUBSCRIPTION.
Dialogs	Indicates the total number of end-to-end SIP signaling connections.
CallID Maps	Indicates the total number of successful session header Call ID mappings.
Rejections	Indicates the total number of rejected INVITEs.
ReINVITEs	Indicates the total number of ReINVITEs.
Media Sessions	Indicates the total number of successful media sessions.
Media Pending	Indicates the total number of media sessions waiting to be established.
Client Trans	Indicates the total number of client transactions.
Server Trans	Indicates the total number of server transactions that have taken place on the Session Director.
Resp Contexts	Indicates the total number of response contexts.
Saved Contexts	Indicates the total number of saved contexts.
Sockets	Indicates the total number of SIP sockets.
Req Drops	Indicates the total number of dropped requests.
DNS Trans	Indicates the total number of Domain Name System (DNS) transactions.
DNS Sockets	Indicates the total number of DNS sockets.
DNS Results	Indicates the total number of DNS results.
Session Rate	Indicates the rate, per second, of SIP invites allowed to or from the Session Director.
Load Rate	Indicates the average CPU utilization of the Session Director.
Active Subscriptions	Indicates the current global count of active SIP subscriptions.

SubscriptionsPerMax	Indicates the maximum global count of SIP subscriptions initiated during any 100 second period since the last Session Director reboot.
Subscriptions High	Indicates the maximum global count of active SIP subscriptions since the last Session Director reboot.

Enabling the Monitoring of SIP Transactions

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the SIP transactions. The page displays the SIP transactions configuration settings for the selected Session Director, under the **SIP Transactions** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of SIP transactions, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.
3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click an active device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.
4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **SIP Transactions** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding Measurement Type, see Configuring the SIP Transactions Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the SIP Transactions setting, go to **Step 5**.
7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the SIP Transactions of the Session Director. The default value is five minutes. You can select only a value that is greater than the default value.
8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing SIP Transactions configuration setting, follow these steps:

1. Select the SIP Transactions configuration that you want to modify and click **Edit**. The **Add/Update Acme SIP Transactions** page opens.
2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing SIP Transactions configuration setting, follow this step:

- Select the SIP Transactions configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing SIP Transactions configuration settings.

To disable an existing SIP Transactions configuration setting, follow this step:

- Select the SIP Transactions configuration that you want to disable, and then click **Disable All**.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the Regional Managers.

Configuring the SIP Transactions Settings

The **Add/Update Acme SIP Transactions** page enables you to define the attributes for configuring the SIP Transactions settings.

To configure SIP Transactions, follow these steps:

1. On the **Add/Update Acme SIP Transactions** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the measurement type that is to be monitored. You can select one of the following types: ▪ **Sessions** ▪ **Subscriptions** ▪ **Dialogs** ▪ **CallID Maps** ▪ **Rejections** ▪ **RelNVITEs** ▪ **Media Sessions** ▪ **Media Pending** ▪ **Client Trans** ▪ **Server Trans** ▪ **Resp Contexts** ▪ **Saved Contexts** ▪ **Sockets** ▪ **Req Drops** ▪ **DNS Trans** ▪ **DNS Sockets** ▪ **DNS Results** ▪ **Session Rate** ▪ **Load Rate** ▪ **Active Subscriptions** ▪ **SubscriptionsPerMax** ▪ **Subscriptions High** **Note:** The **Measurement Type** list also provides the **All** option that

	enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the SIP Transactions type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

Higher Base	Specify the higher base value for the SIP Transactions type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Note: Make sure to add the configuration settings manually to the redundant standby pair of the active Session Director.

Monitoring SIP Client States

You can configure the NNM iSPI for IP Telephony to monitor the statistics of SIP client state. The following table lists the details of the types of measurement attributes that you can configure for monitoring the statistics of SIP client state:

SIP Client States Statistics	Description
All States	Indicates the total number of all the client session transactions.
Initial	Indicates the total number of times the **Initial** state was entered due to the receipt of a request.
Trying	Indicates the total number of times the **Trying** state was entered due to the receipt of a request.
Calling	Indicates the total number of times the **Calling** state was entered due to the receipt of an INVITE request.
Proceeding	Indicates the total number of times the **Proceeding** state was entered due to the receipt of a provisional response while in the **Calling** state.
Cancelled	Indicates the total number of INVITE transactions that received a CANCEL.
EarlyMedia	Indicates the total number of times the **Proceeding** state was entered due to the receipt of a provisional response that contained a Session Description Protocol (SDP) while in the **Calling** state.

Completed	Indicates the total number of times that the **Completed** state was entered due to the receipt of a status code in the range of 300-699 when either in the **Calling** or **Proceeding** state.
Setmedia	Indicates the total number of transactions in which the Session Director was setting up Network Address Translation (NAT) and steering ports.
Established	Indicates the total number of times the client received a 2xx response to an INVITE, but could not forward it because the NAT and steering port information were missing.
Terminated	Indicates the total number of times the **Terminated** state was entered after a 2xx message.

Enabling the Monitoring of SIP Client States

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the SIP client states. The page displays the SIP client states configuration settings for the selected Session Director, under the **SIP Client States** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of SIP client states, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.
3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click an active device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.
4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **SIP Client States** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding Measurement Type, see Configuring the SIP Client States Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the SIP Client States setting, go to **Step 5**.
7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the SIP Client States of the Session Director. The default value is five minutes. You can select only a value that is greater than the default value.
8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing SIP Client States configuration setting, follow these steps:

1. Select the SIP Client States configuration that you want to modify and click **Edit**. The **Add/Update Acme SIP Client States** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing SIP Client States configuration setting, follow this step:

- Select the SIP Client States configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing SIP Client States configuration settings.

To disable an existing SIP Client States configuration setting, follow this step:

- Select the SIP Client States configuration that you want to disable, and then click **Disable All**.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the Regional Managers.

Configuring the SIP Client States Settings

The **Add/Update Acme SIP Client States** page enables you to define the attributes for configuring the SIP Client States settings.

To configure SIP Client States, follow these steps:

1. On the **Add/Update Acme SIP Client States** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the measurement type that is to be monitored. You can select one of the following types: ▪ **All States** ▪ **Initial** ▪ **Trying** ▪ **Calling** ▪ **Proceeding** ▪ **Cancelled** ▪ **EarlyMedia** ▪ **Completed** ▪ **Setmedia** ▪ **Established** ▪ **Terminated** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the SIP Client States type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the SIP Client States type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Note: Make sure to add the configuration settings manually to the redundant standby pair of the active Session Director.

Monitoring SIP Server States

You can configure the NNM iSPI for IP Telephony to monitor the statistics of SIP server state. The following table lists the details of the types of measurement attributes that you can configure for monitoring the statistics of SIP server state:

SIP Server States Statistics	Description
All States	Indicates the total number of all server session transactions.
Initial	Indicates the total number of times the **Initial** state was entered due to the receipt of a request.
Trying	Indicates the total number of times the **Trying** state was entered due to the receipt of a request.
Proceeding	Indicates the total number of times the **Proceeding** state was entered due to the receipt of a provisional response while in the **Calling** state.
Cancelled	Indicates the total number of INVITE transactions that received a CANCEL.
Established	Indicates the total number of times the client received a 2xx response to an INVITE, but could not forward it because the NAT and steering port information were missing.
Completed	Indicates the total number of times that the **Completed** state was entered due to the receipt of a status code in the range of 300-699 when either in the **Calling** or **Proceeding** state.
Confirmed	Indicates the total number of times that an ACK was received while the server was in the **Completed** state and then transitioned to **Confirmed** state.
Terminated	Indicates the total number of times the **Terminated** state was entered after a 2xx message, or never received an ACK in the **Completed** state, and then transitioned to the **Terminated** state.

Enabling the Monitoring of the SIP Server States

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the SIP server states. The page displays the SIP server states configuration settings for the selected Session Director, under the **SIP Server States** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of SIP server states, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.

3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click an active device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.

4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **SIP Server States** from the **Area of Monitoring** drop-down list.

5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding Measurement Type, see Configuring the SIP Server States Settings.

6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the SIP Server States setting, go to **Step 5**.

7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the SIP Server States of the Session Director. The default value is five minutes. You can select only a value that is greater than the default value.

8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing SIP Server States configuration setting, follow these steps:

1. Select the SIP Server States configuration that you want to modify and click **Edit**. The **Add/Update Acme SIP Server States** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing SIP Server States configuration setting, follow this step:

- Select the SIP Server States configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing SIP Server States configuration settings.

To disable an existing SIP Server States configuration setting, follow this step:

- Select the SIP Server States configuration that you want to disable, and then click **Disable All**.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the Regional Managers.

Configuring the SIP Server States Settings

The **Add/Update Acme SIP Server States** page enables you to define the attributes for configuring the SIP Server States settings.

To configure SIP Server States, follow these steps:

1. On the **Add/Update Acme SIP Server States** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the measurement type that is to be monitored. You can select one of the following types: ▪ **Trying** ▪ **Proceeding** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the SIP Server States type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the SIP Server States type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Note: Make sure to add the configuration settings manually to the redundant standby pair of the active Session Director.

Monitoring SIP Invites

You can configure the NNM iSPI for IP Telephony to monitor the statistics of SIP invites. The following table lists the details of the types of measurement attributes that you can configure for monitoring the statistics of SIP invites:

SIP Invites Statistics	Description
INVITE Requests Client Totals	Indicates the total number of client INVITE requests.
INVITE Requests Server Totals	Indicates the total number of server INVITE requests.
Retransmissions Client Totals	Indicates the total number of retransmissions of client INVITEs.
Retransmissions Server Totals	Indicates the total number of retransmissions of server INVITEs.
Response Retrans Client Totals	Indicates the total number of client response retransmissions.
Response Retrans Server Totals	Indicates the total number of server response retransmissions.
Transaction Timeouts Client Totals	Indicates the total number of client INVITE request transaction timeouts.
Locally Throttled Client Totals	Indicates the total number of Client INVITE requests locally throttled.

Enabling the Monitoring of SIP Invites

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the SIP Invites. The page displays the SIP Invites configuration settings for the selected Session Director, under the **SIP Invites** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of SIP invites, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.
3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click an active device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.

4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **SIP Invites** from the **Area of Monitoring** drop-down list.

5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding Measurement Type, see Configuring the SIP Invites Settings.

6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the SIP Invites setting, go to **Step 5**.

7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the SIP Invites of the Session Director. The default value is five minutes. You can select only a value that is greater than the default value.

8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing SIP Invites configuration setting, follow these steps:

1. Select the SIP Invites configuration that you want to modify and click **Edit**. The **Add/Update Acme SIP Invites** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing SIP Invites configuration setting, follow this step:

- Select the SIP Invites configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing SIP Invites configuration settings.

To disable an existing SIP Invites configuration setting, follow this step:

- Select the SIP Invites configuration that you want to disable, and then click **Disable All**.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the Regional Managers.

Configuring the SIP Invites Settings

The **Add/Update Acme SIP Invites** page enables you to define the attributes for configuring the SIP Invites settings.

To configure SIP Invites, follow these steps:

1. On the **Add/Update Acme SIP Invites** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the measurement type that is to be monitored. You can select one of the following types: ▪ **INVITE Requests Client Totals** ▪ **INVITE Requests Server Totals** ▪ **Retransmissions Client Totals** ▪ **Retransmissions Server Totals** ▪ **Response Retrans Client Totals** ▪ **Response Retrans Server Totals** ▪ **Transaction Timeouts Client Totals** ▪ **Locally Throttled Client Totals** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the SIP Invites type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the SIP Invites type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Note: Make sure to add the configuration settings manually to the redundant standby pair of the active Session Director.

Monitoring Session Agents

You can configure the NNM iSPI for IP Telephony to monitor the statistics of the session agents associated with a Session Director. The following table lists the details of the types of measurement attributes that you can configure for monitoring the statistics of Session Agents:

Session Agents Statistics	Description
Inbound Active Sessions	Indicates the total number current, active, inbound sessions.
Inbound Session Rate	Indicates the current inbound session rate in calls per second (CPS).
Outbound Active Sessions	Indicates the total number current, active, outbound sessions.
Outbound Session Rate	Indicates the current outbound session rate in calls per second (CPS).
Inbound Sessions Admitted	Indicates the total number of inbound sessions admitted.
Inbound Sessions Not Admitted	Indicates the total number of inbound sessions rejected because of insufficient bandwidth.
Inbound Concurrent Sessions High	Indicates the highest number of concurrent inbound sessions.
Inbound Average Session Rate	Indicates the average rate of inbound sessions.
Outbound Sessions Admitted	Indicates the total number of outbound sessions admitted.
Outbound Sessions Not Admitted	Indicates the total number of outbound sessions rejected because of insufficient bandwidth.
Outbound Concurrent Sessions High	Indicates the highest number of concurrent outbound sessions.
Outbound Average Session Rate	Indicates the average rate of outbound sessions.
Max Burst Rate	Indicates the burst rate of traffic (both inbound and outbound) measured.
Total Seizures	Indicates the total number of seizures.
Total Answered Sessions	Indicates the total number of answered sessions.
Answer/Seizure Ratio	Indicates the percentage of answer-to-seizure ratio.

Average One-Way Signaling Latency	Indicates the average observed one-way signaling latency.
Maximum One-Way Signaling Latency	Indicates the maximum observed one-way signaling latency.

Enabling the Monitoring of Session Agents

The **Monitoring Configuration for Acme SBC** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the Session Agents associated with a Session Director. The page displays the Session Agents configuration settings for the selected Session Director, under the **Session Agents** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of Session Agents, follow these steps:

1. From the NNMi console, click the **Acme IP Telephony** workspace in the left pane.
2. Click **Session Director**. The Acme Session Director view opens.
3. Select an active device from the Acme Session Director view and click **Actions** > **IP Telephony** > **Monitoring Configuration**. (Alternatively, right-click a device in the Acme Session Director view, and then click **IP Telephony > Monitoring Configuration**.) The **Monitoring Configuration for Acme SBC** page opens.
4. On the left pane of the **Monitoring Configuration for Acme SBC** page, select **Session Agents** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding Measurement Type, see Configuring the Session Agents Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the Session Agents setting, go to **Step 5**.
7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the Session Agents associated with the Session Director. The default value is five minutes. You can select only a value that is greater than the default value.
8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing Session Agents configuration setting, follow these steps:

1. Select the Session Agents configuration that you want to modify and click **Edit**. The **Add/Update Acme Session Agents**page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing Session Agents configuration setting, follow this step:

- Select the Session Agents configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing Session Agents configuration settings.

To disable an existing Session Agents configuration setting, follow this step:

- Select the Session Agents configuration that you want to disable, and then click **Disable All**.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the regional managers.

Configuring the Session Agents Settings

The **Add/Update Acme Session Agents** page enables you to define the attributes for configuring the Session Agents settings.

To configure Session Agents, follow these steps:

1. On the **Add/Update Acme Session Agents** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the measurement type that is to be monitored. You can select one of the following types: ▪ **Inbound Active Sessions** ▪ **Inbound Session Rate** ▪ **Outbound Active Sessions** ▪ **Outbound Session Rate** ▪ **Inbound Sessions Admitted** ▪ **Inbound Sessions Not Admitted** ▪ **Inbound Concurrent Sessions High** ▪ **Inbound Average Session Rate** ▪ **Outbound Sessions Admitted** ▪ **Outbound Sessions Not Admitted** ▪ **Outbound Concurrent Sessions High** ▪ **Outbound Average Session Rate** ▪ **Max Burst Rate** ▪ **Total Seizures** ▪ **Total Answered Sessions** ▪ **Answer/Seizure Ratio** ▪ **Average One-Way Signaling Latency** ▪ **Maximum One-Way Signaling Latency** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.

Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the Session Agents type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the Session Agents type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.

Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Note: Make sure to add the configuration settings manually to the redundant standby pair of the active Session Director.

Avaya IP Telephony

The Avaya IP Telephony workspace enables you to view the inventory views for the Avaya devices and entities that are discovered and monitored in your environment. The following table lists the options that you can click to view the details of a discovered device or an entity:

Inventory View	Purpose
Call Controllers	Lists the Avaya Call Controllers discovered on the network.
IP Phones	Lists the Avaya IP Phones discovered on the network.
Media Gateways	Lists the Avaya Media Gateways discovered on the network.

Monitoring Avaya Call Controllers

The Call Controllers view displays a list of available Avaya Call Controllers on the network. The view arranges the key attributes of all discovered Avaya Call Controllers in a table.

To launch the Avaya Call Controllers view:

From the **Workspaces** navigation pane, click **Avaya IP Telephony > Call Controllers**. The Call Controllers view opens in the right pane.

Basic Attributes of the Avaya Call Controllers Table

Attribute	Description
State	Indicates the state of the call controller. The state can be one of the following: • Active—indicates the call controller is in the active state. • Standby—indicates that the call controller is in the standby state. • Unknown—indicates that the status of the call controller is currently unknown.

Basic Attributes of the Avaya Call Controllers Table, continued

Attribute	Description
Fault State	Indicates the state of the system based on the calculation done with SNMP traps that originate from Avaya maintenance objects (MOs).
Name	Indicates the name of the call controller.
IP Address	Indicates the IP address of the call controller.
Tenant	Indicates the name of the tenant to which the call controller belongs.
Type	Indicates the type of the call controller. The type can be one of the following: • Primary Server—indicates that the call controller is a primary server. • LSP—indicates that the call controller is a Local Survivable Processor (LSP).
Version	Indicates the version of the call controller.
Management Server	The management server for the Call Controller. This attribute displays one of the following values: • **Local**: If the call controller is being managed by the NNMi management server console on which you are viewing the call controller details. • Name of the regional manager that manages the call controller.

To view the Avaya Call Controller Form:

In the Call Controllers view, select the call controller of interest and then click . The Avaya Call Controller Details Form opens.

To view the node form for the call controller, click and click **Open**. The Node form opens and displays the details of the call controller.

Analysis Pane

The Analysis pane displays a summary of the details of the selected call controller as follows:

Avaya Call Controller Details Summary tab

- Name: The name of the selected call controller.
- Management Address: The external (public) IP address of the call controller.
- Tenant: The name of the tenant to which the call controller belongs.
- Management Server: The management server for the Call Controller. This attribute displays one of the following values:
  - Local: If the call controller is being managed by the NNMi management server console on which you are viewing the call controller details.
  - Name of the regional manager that manages the call controller.

General Information tab

- Management Mode: The management state of the call controller. The status can be one of the following strings: Managed, Unmanaged, or Out of Service.
- Type: Indicates the type of the call controller: Primary Server or LSP.
- Model: The model of the call controller.
- Version: The version of the call controller.
- Time Zone: The time zone configured for the call controller.
- State: Indicates the state of the call controller. The state can be one of the following values: Active, Standby, or Unknown.
- Duplicated Server: The IP address of duplicate server paired with the primary server.
- Description: The description of the call controller.
- Location: The location of the call controller.
- Fault State: Indicates the state of the call controller based on the calculation done with SNMP traps that originate from Avaya Communication Manager on different Maintenance Objects (MOs). The possible values are: Warning, Minor, Major and Clear.
- CLAN G3 Alarm Summary: The summary of G3 alarms along with the severities received from the Control LANs associated with the call controller.
- MedPro G3 Alarm Summary: The summary of G3 alarms along with the severities received from the media processors associated with the call controller.
- IPSI G3 Alarm Summary: The summary of G3 alarms along with the severities received from the IP server interfaces associated with the call controller.
- H.248 MGW G3 Alarm Summary: The summary of G3 alarms along with the severities received from the H.248 media gateways associated with the call controller.

Device Registrations tab

- Registered IP Phone Extensions: The number of IP phones registered with the selected call controller.
- Registered H248 Media Gateways: The number of H248 gateways associated with the selected call controller.

IP Phone Registrations tab

Under the IP Phone Registrations tab, you can see the status of all the IP phones registered with the selected call controller in a pie chart. The possible values for the status are as follows:

- Registered
- Unregistered
- Unknown
- Rejected
- Partially Registered

Filtering Avaya Call Controllers

You can filter the listed call controllers in the Call Controllers view based on the following attributes of the Call Controller:

- State
- Name
- IP Address
- Tenant
- Type
- Version
- Management Server

Note: You can create filters for each of the listed attributes to view only the required Call Controllers.

To filter the Call Controllers view:

1. Right-click any of the listed attribute columns of one of the call controllers listed in the Call Controllers view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the call controllers that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the call controllers for which the selected column is not empty.
   - **Is empty**: filters and lists all the call controllers for which the selected column is empty.

- **Not equal to this value**: filters and lists all the call controllers that do not have the value in the column that you selected.

  The filtered list of call controllers appears in the view.

All the attributes that you can use to filter are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to use to filter.

You can also filter the Call Controllers by right clicking the attribute column headings and selecting **Filter** and one of the following options:

- Is not empty
- Is empty
- Create Filter

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Avaya Call Controller Details Form

The Avaya Call Controller Details Form is split into two panes, the right pane and the left pane. The right pane lists the following details:

- IP Phones: This tab displays the list of IP phones configured with the selected Avaya Call Controller. The tab displays the details of the IP phones in the format specified in the IP Phones view.
- Port Network: This tab displays the list of port networks as displayed in the port networks view.
- Duplicated Server: This tab displays the attributes of the duplicate server paired with the primary server as shown in the Monitoring Avaya Call Controllers page.
- Survivable Servers: This tab displays the attributes of the configured local survivable processor as shown in the Monitoring Avaya Call Controllers page.
- Primary Controllers: This tab displays the attributes of the primary call controller as shown in the Monitoring Avaya Call Controllers page.
- Network Regions: This tab displays the attributes of the configured network regions as shown in the Monitoring Network Regions page.
- Route Patterns: This tab displays the attributes of the configured route patterns as shown in the Monitoring Route Patterns page.

- Trunk Groups: This tab displays the details of the configured trunk groups as shown in the Monitoring Trunk Groups page.
- Signaling Groups: This tab displays the details of the configured signaling groups as shown in the Monitoring Signaling Groups page.
- Occupancy: This tab displays the call controller processor utilization metrics by different processes for the past one hour during which the processor utilization metrics were collected. You can specify threshold values for the different processes. as shown in the Monitoring Processor Occupancy page.
- Media Gateways: This tab displays the details of the media gateway associated with the call controller as shown in the Monitoring Media Gateways page.
- Incidents: This tab displays the incidents generated for the processes that violated the specified threshold.

The left pane lists the attributes of the call controller in a tabular form.

General Attributes of the Call Controller

Attribute	Description
Hosted Node	The node on which the call controller is hosted.
Name	The name of the call controller.
IP Address	The IP address of the call controller.
Type	The type of the call controller.
Management Mode	Displays the management state of the Call Controller. The status can be one of the following strings: • Managed: indicates that the node is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the node is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the NNM iSPI for IP Telephony.
Model	The model of the call controller.
Version	The version of the call controller.
Hardware	The hardware type of the call controller.
Load Number	The call controller load number.

General Attributes of the Call Controller, continued

Attribute	Description
Release Number	Specifies the release number of the call controller.
Operating System	The operating system running on the call controller.
Description	The description of the call controller.
Domain	The domain name of the call controller.
Location	The location of the call controller.
Time Zone	The time zone configured for the call controller.

Primary Server Attributes

Attribute	Description
State	The state of the primary server.
Duplicated Server	The IP address of duplicate server paired with the primary server.
Virtual Name	The virtual name of the primary server.
Virtual IP Address	The virtual IP address of the primary server.

Survivable Server Specific Attributes

Attribute	Description
Primary	The IP address of the configured survivable processor.
Processor ID	The ID of the configured survivable processor.
Network Region	The network region to which the survivable processor belongs.
Registered to Primary	Indicates if the survivable processor is registered with the primary controller. The value can be Yes or No.
Is Active	Indicates if the survivable processor is in the active state or not. The value can be Yes or No.

Analysis Pane

The Analysis pane displays a summary of the details of the selected call controller.. For more information, see Monitoring Avaya Call Controllers.

Monitoring Network Regions

The Network Regions tab page displays the network regions associated with the call controller. The page displays the following details.

Attributes of the Network Regions

Attribute	Description
Number	The network region number.
Name	The name of the network region.

You can view the details of a single network region in a form.

To view the IP Network Region Detail form:

Select the network region of your interest, and then click . The IP Network Region Detail Form opens.

Analysis Pane

The Analysis pane displays a summary of the details of the selected network region as follows:

IP Network Region Details Summary tab

- Name: The name of the network region.
- Call Server: The call controller that controls the network region.
- Management Server: The management server for the network region. This attribute displays one of the following values:
  - Local: If the network region is being managed by the NNMi management server console on which you are viewing the network region details.
  - Name of the regional manager that manages the network region.

Avaya IP Network Region Information tab

- Number: The network region number.
- Number of Connections: The number of other network regions connected with the selected network region.
- Number Of IP Media Processor DSP Resources: The number of IP media processor DSP resources on the selected network region.
- Number of MedPro: The number of media processors associated with the selected network region.

- Number of Media Gateway: The number of media gateways associated with the selected network region.
- RSVP Enabled: Indicates if Resource Reservation Protocol (RSVP) is enabled on the selected network region.

Filtering Avaya Network Regions

You can filter the listed network regions in the Network Regions tab page based on the following attributes of the network region:

- Number
- Name

Note: You can create filters for each of the listed attributes to view only the required network regions.

To filter the network regions:

1. Right-click any of the listed attribute columns of one of the network regions listed in the Network Regions tab page and select **Filter**.
2. Select one of the following filter options:
   - **Equals this value**: filters and lists all the network regions that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the network regions for which the selected column is not empty.
   - **Is empty**: filters and lists all the network regions for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the network regions that do not have the value in the column that you selected.

     The filtered list of network regions appears in the view.

   You can also filter the network regions by right clicking the attribute column headings and selecting **Filter** and one of the following options to filter the network regions:
   - Is not empty
   - Is empty
   - Create Filter

The **Name** attribute that you can use to filter is case sensitive. Make sure that you use the correct character case to specify the attribute value.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

IP Network Region Detail Form

The IP Network Region Detail form is split into two panes. The right pane displays the following details:

- IP Media Processor DSP Resources: This tab page displays the metrics that denote the usage of the IP media processor resources in the network region as shown on the Monitoring IP Media Processor DSP Resource Metrics page.
- Connections: This tab page displays the other network regions connected with the network region as shown on the Monitoring IP Network Regions Connections page.
- Incidents: This tab page displays the incidents related to the network region.
- MedPros: This tab page displays the details of the media processors associated with the network region as shown on the Monitoring Media Processors page.
- Media Gateways: This tab page displays the details of the media gateways associated with the network region as shown on the Monitoring Avaya Media Gateways page.

The left pane lists the following general attributes for the network region.

General Attributes of the Network Region

Attribute	Description
Name	The name of the network region.
Number	The network region number.
Number of IP Media Processor DSP Resources	The number of IP media processor DSP resources on the network region.
DiffServ/TOS Call Control PHB	The Differentiated Services/Type of Services (DiffServ/TOS) Call Control parameter Per-Hop Behavior (PHB) value for the network region.
DiffServ/TOS Voice PHB	The DiffServ/TOS voice parameter PHB value.
Call Control 802.1p Priority	The call control 802.1p priority value for the network region.

General Attributes of the Network Region, continued

Attribute	Description
Voice 802.1p Priority	The voice 802.1p priority value for the network region.
Is RSVP Enabled	Indicates if Resource Reservation Protocol (RSVP) is enabled on the port network.
RSVP Refresh Rate	Displays the RSVP refresh rate specified.
Retry on RSVP Failure	Indicates if the feature to retry on RSVP failure is enabled on the port network.
RSVP Profile	Lists the RSVP profile. The profile can be one of the following: • controlled-load • guaranteed-service
RSVP Unreserved BBE PHB	The RSVP unreserved Better than Best Effort (BE) (BBE) PHB value for the network region.

Monitoring IP Media Processor DSP Resource Metrics

This tab page displays the metrics that denote the usage of the IP media processor resources in the network region. You can view the metric values and specify threshold values based on your requirements for each of the metrics. The page displays the following metrics.

IP Media Processor DSP Resource Metrics

Metric	Description
DSP Usage (Erlangs)	Lists the amount of time in Erlangs when all the codecs (voice channels) were in use in the network region when this metric was collected. The time measured includes the time the voice channel was allocated to the time the voice channel was released after the call. The threshold range that you can specify is from 0-9999.
In Region Allocations Peg	Lists the number of times an IP media processor port in the network region was allocated for a call. The threshold range that you can specify is from 0-65535.
Out of Region Allocations Peg	Lists the number of times an IP media processor port in the network region was required for a call, but was then allocated to a call in another network region. The threshold range that you can specify is from 0-65535.

IP Media Processor DSP Resource Metrics, continued

Metric	Description
Allocations Denied Peg	Lists the number of times an IP media processor port in the network region was required for a call, but could not be allocated to the call. The reason for this might be that all the ports in all the network regions were busy thus causing the call connection to be unsuccessful. The threshold range that you can specify is from 0-65535.
% Blocked	Lists the percentage of codecs that are busy in the network region. (Clarify)
% Out of Service (CCS)	List the percentage of codecs in the network region that are out of service. (Clarify)
G711 Usage (Erlangs)	Lists the amount of time in Erlangs when all the G711 codecs (voice channels) were in use in the network region when this metric was collected. The time measured includes the time the voice channel was allocated to the time the voice channel was released after the call.
G711 In Region Allocations Peg	Lists the number of times an IP media processor port in the network region was allocated for a G711 call. The threshold range that you can specify is from 0-65535.
G711 Out of Region Allocations Peg	Lists the number of times an IP media processor port in the network region was required for a G711 call, but was then allocated to a call in another network region.
G723/G729 Usage (Erlangs)	Lists the amount of time in Erlangs when all the G723 or G729 codecs (voice channels) were in use in the network region when this metric was collected. The time measured includes the time the voice channel was allocated to the time the voice channel was released after the call.
G723/G729 In Region Allocations Peg	Lists the number of times an IP media processor port in the network region was allocated for a G723 or a G729 call. The threshold range that you can specify is from 0-65535.
G723/G729 Out of Region Allocations Peg	Lists the number of times an IP media processor port in the network region was required for a G723 call or a G729 call, but was then allocated to a call in another network region.

Specifying Threshold Values for Metrics

You can specify the required threshold values for the metrics listed in the table to measure and monitor if the metric is within the threshold value you specified.

To specify a threshold value, do as follows:

1. Specify a threshold value for the required metric in the **Threshold Value** box for that metric.
2. Click **Save and Close** from the menu bar to apply the threshold value for the metric. After the next hour, the NNM iSPI for IP Telephony compares the metric with the specified value. If the value exceeds the specified threshold value, the NNM iSPI for IP Telephony generates an incident on the Incidents tab page of the Avaya Call Controller form.

IP Network Region Connection Detail Form

The IP Network Region Connection Detail form is split into two panes. The right pane displays the following details:

- Connected Regions: This tab page displays the details of the network regions connected to the network region as shown on the Monitoring Network Regions page. You can select a network region and click to open the IP Network Region Detail form for that port network.
- Incidents: This tab page displays the details of the media gateways associated with the network region as shown on the Monitoring Avaya Media Gateways page.

The left pane lists the following general attributes for the connected network region.

General Attributes of the Connected Network Region

Attribute	Description
Status	The status of the connection. The status can be any of the following: • Pass • Fail
Name	The name of the IP network region.
Source	The IP network region that serves as the source of the VOIP traffic.
Destination	The IP network region that serves as the destination for VOIP traffic.
Type	The type of connection. This value can be one of the following: • Direct • Indirect
Denial Count	The value of the denial count.
Denial Count Threshold	You can specify the value for the denial count threshold in the box provided. You must click the **Save and Close** icon from the menu to apply this threshold setting.

General Attributes of the Connected Network Region, continued

Attribute	Description
Transmit Bandwidth Used for Direct Connections	The transmit bandwidth used for direct connections
Receive Bandwidth Used for Direct Connections	The receive bandwidth used for direct connections.
Transmit Connection Count	The value of the transmitted connection count for direct connections.
Receive Connection Count	The value of the received connection count for direct connections.
Administered Bandwidth Value	The administered bandwidth value.

Monitoring Route Patterns

The Route Patterns tab page displays the route patterns available on the call controller. The page displays the following details about the route patterns:

Attributes of the Route Pattern

Attribute	Description
Pattern Number	The unique identification number for the route pattern.
First Trunk Group Number	The unique identification number for the first trunk group associated with .the route pattern.

You can view the details of a single route pattern in a form.

To view the Route Pattern Detailed form:

Select the route pattern of your interest, and then click . The Route Pattern Detailed form opens.

Analysis Pane

The Analysis pane displays a summary of the details of the selected route pattern as follows:

Route Pattern Details Summary tab

- Pattern Number: The unique identification number for the route pattern.
- Controller: The IP address of the call controller that controls the route pattern.

- Management Server: The management server for the route pattern. This attribute displays one of the following values:
  - Local: If the route pattern is being managed by the NNMi management server console on which you are viewing the route pattern details.
  - Name of the regional manager that manages the route pattern.

Avaya Route Pattern Information tab

- Management Mode: The management state of the route pattern. The status can be one of the following strings: Managed, Unmanaged, or Out of Service.
- First Trunk Group Number: The unique identification number for the first trunk group associated with the selected route pattern.
- Number of Trunk Group Members In Service: Indicates the total number of trunk group members in the service.
- Number of Trunk Groups: The number of trunk groups associated with the selected route pattern.

Filtering Avaya Route Patterns

You can filter the listed route patterns in the Route Patterns tab page based on the following attributes:

- Pattern Number
- First Trunk Group Number

Note: You can create filters for each of the listed attributes to view only the required route patterns.

To filter the Route Patterns tab page view:

1. Right-click any of the listed attribute columns of one of the route patterns listed in the Route Patterns tab page view and select **Filter**.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the route patterns that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the route patterns for which the selected column is not empty.
   - **Is empty**: filters and lists all the route patterns for which the selected column is empty.

- **Not equal to this value**: filters and lists all the route patterns that do not have the value in the column that you selected.

  The filtered list of route patterns appears in the view.

You can also filter the route patterns by right clicking the attribute column headings and selecting **Filter** and one of the following options:

- Is not empty
- Is empty
- Create Filter

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Route Pattern Details Form

The Route Pattern Details form is split into two panes. The right pane lists the following details about the route pattern:

- Trunk Groups: displays the details of the trunk groups associated with the route pattern as shown on the Monitoring Trunk Groups page. You can select a trunk group and click to view the Trunk Group Detailed form for that trunk group.
- Incidents: displays the incidents related to the route pattern.

The left pane lists the following general attributes and the usage details for the selected route pattern.

General Attributes of the Route Pattern

Attribute	Description
Hosted Node	The host name for the route pattern. To view the Node Form for the route pattern, click , and then click **Open**. The Node Form, displaying the details of the route pattern, opens.
Pattern No.	The unique identification number for the route pattern.
First Trunk Group No.	The unique identification number for the first trunk group associated with .the route pattern.

General Attributes of the Route Pattern, continued

Attribute	Description
Management Mode	Displays the management state of the route pattern. The status can be one of the following strings: • Managed: indicates that the route pattern is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the route pattern is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the route pattern is currently not managed by the NNM iSPI for IP Telephony.
Total Members in Service	Indicates the total number of members in the service.
Free Members in Service	Indicates the free members in the service.

Usage Details for the Route Pattern

Attribute	Description
Queue Size	The length of the queue for the first trunk group in the route pattern.
Queue Size Threshold	The text box to specify the queue size threshold value.
Calls Offered	The total number of calls offered to the route pattern.
Calls Offered Threshold	The text box to specify the calls offered threshold value.
Calls Carried	The total number of seizures (resources in the trunk groups used) by calls for all the trunk groups in the route pattern.
Calls Carried Threshold	The text box to specify the calls carried threshold value.
Calls Blocked	The total number of calls that could not get a trunk group allocation due to a trunk group busy state in the route pattern.
Calls Blocked Threshold	The text box to specify the calls blocked threshold value.

Attribute	Description
Calls Queued	The number of calls that were placed in the queue of the first trunk group in the route pattern as all the trunk groups in the route pattern were busy to be allocated for the calls.
Calls Queued Threshold	The text box to specify the calls queued threshold value.
Queue Overflow	The number of calls that could not be queued in the first trunk group queue as the queue was already full.
Queue Overflow Threshold	The text box to specify the queue overflow threshold value.

Note: To apply a threshold value, click (the **Save** icon) on the menu bar after you specify the value in the respective box.

Note: The NNM iSPI for IP Telephony generates an incident in the incident inventory during a threshold violation. However, the incident is canceled if the attribute value is within the set threshold in the next polling. Multiple incidents are not generated for consecutive threshold violations of a single attribute value. For example, if the **Queue Size** threshold value is violated for consecutive polling, the incident inventory continues to display the incident generated after the first violation and cancels it only when the value is within the set threshold.

Monitoring Trunk Group Usage

The Trunk Group Usage tab page displays the trunk group usage details on the route pattern. The page displays the following details.

Trunk Group Usage Details

Attribute	Description
Group No.	Specifies the trunk group number.
% Calls Carried	The total percentage of calls carried by a trunk group in the route pattern.
Total Calls	The total number of calls carried by a trunk group in the route pattern.

You can select a trunk group from this tab page and click to view the Trunk Group Detailed form for that trunk group.

Monitoring Trunk Groups

The Trunk Groups tab page displays the trunk groups associated with the call controller. The page displays the attributes of the trunk group as shown in the following table.

Attributes of the Trunk Groups

Attribute	Description
Group Number	Indicates the trunk group number.
Type	Indicates the trunk group type.
Name	Indicates the name of the trunk group.
Service Type	Indicates the trunk group service type.
Custom Info	Indicates the custom information configured for the trunk group.
Size	Indicates the number of trunk group members in the trunk group.

You can view the details of a single trunk group in a form.

To view the Trunk Group Detailed form:

Select the trunk group of your interest, and then click . The Trunk Group Detailed form opens.

Analysis Pane

The Analysis pane displays a summary of the details of the selected trunk group as follows:

Trunk Group Details Summary tab

- Name: The name of the trunk group.
- Management Server: The management server for the trunk group. This attribute displays one of the following values:
  - Local: If the trunk group is being managed by the NNMi management server console on which you are viewing the trunk group details.
  - Name of the regional manager that manages the trunk group.

Avaya Trunk Group Information tab

- Management Mode: The management state of the trunk group. The status can be one of the following strings: Managed, Unmanaged, or Out of Service.
- Direction: The trunk group direction.
- Service Type: The trunk group service type.
- Size: The number of trunk group members in the trunk group.

- Total Members in Service: The total members in service for the trunk group.
- Number of Route Patterns Referencing this Trunk Group: The number of route patterns associated with the selected trunk group.

Filtering Avaya Trunk Groups

You can filter the listed trunk groups in the Trunk Groups tab page based on the following attributes:

- Group Number
- Type
- Name
- Service Type
- Custom Info
- Size

Note: You can create filters for each of the listed attributes to view only the required trunk groups.

To filter the Trunk Groups tab page view:

1. Right-click any of the listed attribute columns of one of the trunk groups listed in the Trunk Groups tab page view and select **Filter**.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the trunk groups that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the trunk groups for which the selected column is not empty.
   - **Is empty**: filters and lists all the trunk groups for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the trunk groups that do not have the value in the column that you selected.

     The filtered list of trunk groups appears in the view.

   You can also filter the trunk groups by right clicking the attribute column headings and selecting **Filter** and one of the following options:

- Is not empty
- Is empty
- Create Filter

All the attributes that you can use to filter are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to use to filter.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Trunk Group Detailed Form

The Trunk Group Detailed form is split into two panes. The right pane lists the following details about the selected trunk group:

- Members: displays the trunk group members that belong to the trunk group as shown on the Monitoring Trunk Group Members page.
- Route Patterns: displays the route patterns associated to the trunk group as shown on the Monitoring Route Patterns page. You can select a route pattern and click to see the Route Pattern Detailed form for the selected route pattern.

The left pane displays the general attributes and the usage details of the selected trunk group as shown in the following tables:

General Attributes of the Trunk Group

Attribute	Description
Hosted Node	The host name of the trunk group. To view the Node Form for the trunk group, click , and then click **Open**. The Node Form, displaying the details of the trunk group, opens.
Group No.	The trunk group number.
Type	The trunk group type.
Name	The name of the trunk group.
Size	The number of trunk group members in the trunk group.
Direction	The trunk group direction.
Service Type	The trunk group service type.
Signaling Type	The trunk group signaling type.

General Attributes of the Trunk Group, continued

Attribute	Description
Communication Type	The trunk group communication type.
Total Members In Service	The total members in service for the trunk group.
Free Members In Service	The free members in service for the trunk group.
Custom Info	The custom information configured for the trunk group. You can type the custom information required for the Trunk Group and click (the **Save** icon) to save the custom information for the Trunk Group.
Access Code	The access code configured for the trunk group.

Usage Details of the Trunk Group

Attribute	Description
Total Seize	Indicates the total number of times a trunk was seized in the group.
Total Seize Threshold	The text box to specify the total seize threshold value.
Incoming Seize	The total number of incoming seizures on the trunk group.
Incoming Seize Threshold	The text box to specify the incoming seizure threshold value.
Group Overflow	The total number of calls to a trunk group that were not placed in a queue or carried.
Group Overflow Threshold	The text box to specify the group overflow threshold value.
Queue Size	The number of slots assigned to the trunk group queue.
Queue Size Threshold	The text box to specify the queue size threshold value.
Queue Overflow	The total number of calls that were not queued as the queue was full.
Queue Overflow Threshold	The text box to specify the queue overflow threshold value.
Queue Abandoned	The total number of calls that were removed from the queue.
Queue Abandoned Threshold	The text box to specify the queue abandoned threshold value.

Attribute	Description
Out of Service	The total number of trunks in the trunk group that are out of service due to maintenance.
Out of Service Threshold	The text box to specify the out of service threshold value.
%ATB	The percentage of the time when all the trunks in the group were busy.
%ATB Threshold	The text box to specify the ATB percentage threshold value.
%Out Block	The percentage of the calls that were offered to the trunk group, but was not carried on the trunk group.
%Out Block Threshold	The text box to specify the out block percentage threshold value.

Note: To apply a threshold value, click (the **Save** icon) on the menu bar after you specify the value in the respective box.

Note: The NNM iSPI for IP Telephony generates an incident in the incident inventory during a threshold violation. However, the incident is canceled if the attribute value is within the set threshold in the next polling. Multiple incidents are not generated for consecutive threshold violations of a single attribute value. For example, if the **Queue Size** threshold value is violated for consecutive polling, the incident inventory continues to display the incident generated after the first violation and removes it only when the value is within the set threshold.

Monitoring Trunk Group Members

The Members tab page displays the trunk group member details as shown in the following table.

Trunk Group Member Details

Attribute	Description
Service State	Indicates the service state of the trunk group member.
Group No.	Specifies the trunk group number that includes the member.
Group Member No.	Displays the trunk group member number.
Port	Displays the trunk port of the trunk group member.
Signaling Group No.	Displays the signaling group number assigned to the trunk group member.

You can select a trunk group from this tab page and click to view the Trunk Group Member Detailed form for that trunk group member.

Trunk Group Member Detailed Form

The Trunk Group Member Detailed form is split into two panes. The right pane lists the following details as tab pages:

- Signaling Group: displays the signaling groups associated with the trunk group as shown on the Monitoring Signaling Groups page.
- Incidents: displays the incidents specific to the trunk group member.

The left pane lists the general attributes and the state of the trunk group member as shown in the following tables.

General Attributes of Trunk Group Member

Attribute	Description
Hosted Node	The host name of the trunk group member. To view the Node Form for the trunk group member, click , and then click **Open**. The Node Form opens displaying the details of the trunk group member.
Group Member No.	The trunk group member number.
Name	The name of the trunk group member.
Type	The trunk group member type.
Port	The trunk port of the trunk group member.
Group No.	The trunk group number that includes the member.
Signaling Group No.	The signaling group number assigned to the trunk group member.

State Attributes of Trunk Group Member

Attribute	Description
Maintenance Busy	Indicates whether the trunk group member state is busy for maintenance.
Service State	Indicates the service state of the trunk group member.

Monitoring Signaling Groups

The Signaling Groups tab page displays a list of available signaling groups associated with the call controller. The page displays the following details.

Attributes of the Signaling Groups

Attribute	Description
Service State	The service state of the signaling group.
Signaling Group Number	The number that uniquely identifies the signaling group on the call controller.
FAS	Indicates whether Facility-associated Signaling (FAS) is enabled for the signaling group.
Primary D Channel	The unique identifier for the primary D channel administered for the signaling group.
Secondary D Channel	The unique identifier for the secondary D channel administered for the signaling group.

You can view the details of a single signaling group in a form.

To view the Signaling Group Details Form:

Select the signaling group of your interest, and then click . The Signaling Group Details Form opens.

Analysis Pane

The Analysis pane displays a summary of the details of the selected signaling group as follows:

Signaling Group Details Summary tab

- Signaling Group Number: The number that uniquely identifies the signaling group on the call controller.
- Management Server: The management server for the signaling group. This attribute displays one of the following values:
  - Local: If the signaling group is being managed by the NNMi management server console on which you are viewing the signaling group details.
  - Name of the regional manager that manages the signaling group.

Avaya Signaling Group Information tab

- Management Mode: The management state of the signaling group. The status can be one of the following strings: Managed, Unmanaged, or Out of Service.
- Service State: The service state of the signaling group.
- Number of Trunk Group Members using this Signaling Group

Signaling Group Details Form

The Signaling Group Detailed form is split into two panes. The right pane displays the following details as tab pages:

- Trunk Group Members: displays the trunk group members associated with the signaling group as shown on the Monitoring Trunk Group Members page. You can select a trunk group member and click to open the Trunk Group Member Detailed form.
- Incidents: displays the incidents related to the selected signaling group.

The left pane displays the general attributes and the state of the signaling group as shown in the following tables.

General Attributes of the Signaling Group

Attribute	Description
Hosted Node	The hostname of the signaling group.
Signaling Group No.	The number that uniquely identifies the signaling group.
FAS	Indicates whether Facility-associated Signaling (FAS) is enabled for the signaling group.
Primary D Channel	The unique identifier for the primary D channel administered for the signaling group.
Secondary D Channel	The unique identifier for the secondary D channel administered for the signaling group.

State Attribute of the Signaling Group

Attribute	Description
Service State	The service state of the signaling group.

To view the Node Form for the signaling group, click , and then click **Open**. The Node Form opens displaying the details of the signaling group.

Monitoring Processor Occupancy Metrics

The Occupancy tab page displays the Avaya call controller processor utilization metrics. This tab page displays the processor utilization metrics based on the processes that utilize the processor. The page displays the metrics for the last hour. You can view the processor metrics, specify the threshold values for the processor metrics, and see the current metric value to determine the metrics that violate the specified threshold value.

See the following table to know more about the metrics.

Metric	Description
Static (%)	The percentage of processor utilization by static processes.

Metric	Description
Call Processing (%)	The percentage of processor utilization by call processing processes.
System Management (%)	The percentage of processor utilization by system management processes.
Idle (%)	The percentage of processor utilization that is not used.
Total Calls	The total calls connected during the last hour.
Tandem Calls	The total calls connected during the last hour between trunks.
Total Call Attempts	The total calls attempted during the last hour.
Intercom Attempts	The total calls attempted from extension on the same switch during the last hour.
Incoming Attempts	The total number of incoming trunk slots used (seizures) on the call controller by public networks.
Outgoing Attempts	The total outgoing seizures on the call controller using public networks.
Private Network Attempts	The total number of incoming and outgoing seizures over private networks.

Specifying Threshold Values for Metrics

You can specify the required threshold values for the metrics listed in the table to measure and monitor if the metric is within the threshold value you specified.

To specify a threshold value, do as follows:

1. Specify a threshold value for the required metric in the **Threshold Value** box for that metric.
2. Click **Save and Close** from the menu bar to apply the threshold value for the metric. After the next hour, the NNM iSPI for IP Telephony compares the metric with the specified value. If the value exceeds the specified threshold value, the NNM iSPI for IP Telephony generates an incident on the Incidents tab page of the Avaya Call Controller form.

Monitoring Avaya Port Networks

Basic Attributes of the Port Networks Table

Attribute	Description
Number	Denotes the port network number and the IP address of the call controller that controls the port network.

Basic Attributes of the Port Networks Table, continued

Attribute	Description
IPSI A IP Address	Denotes the IP address of the IP Server Interface (IPSI) A board on the port network.
IPSI A Service State	Displays the service state of the IPSI A board. The service state can be one of the following: • In: denotes that the service state is active. • Out: denotes that the service state is inactive.
IPSI B IP Address	Denotes the IP address of the IP Server Interface (IPSI) B board on the port network.
IPSI B Service State	Displays the service state of the IPSI B board. The service state can be one of the following: • In: denotes that the service state is active. • Out: denotes that the service state is inactive.

You can view the details of a port network and the associated devices in the Port Network Details Form.

To view the Port Network Details Form:

In the Port Networks view, select the node of your interest, and then click . The Port Network Details Form opens.

Analysis Pane

The Analysis pane displays a summary of the details of the selected port network as follows:

Port Network Details Summary tab

- Number: The port network number.
- Controller: The call controller that controls the port network.
- Management Server: The management server for the port network. This attribute displays one of the following values:
  - Local: If the port network is being managed by the NNMi management server console on which you are viewing the port network details.
  - Name of the regional manager that manages the port network.

Avaya Port Information tab

- Number of CLAN: The number of CLANs associated with the port network.
- Number of IPSI: The number of IPSI boards on the port network.

- Number of MedPro: The number of media processors associated with the port network.

Filtering Avaya Port Networks

You can filter the listed port networks in the Port Networks view based on the management server.

To filter the Port Networks view:

1. Right-click the **Management Server** attribute column of one of the port networks listed in the Port Networks view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the port networks that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the port networks for which the selected column is not empty.
   - **Is empty**: filters and lists all the port networks for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the port networks that do not have the value in the column that you selected.

     The filtered list of port networks appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Port Network Detail Form

The Port Network detail form is split into two panes, the right pane and the left pane. The right pane lists the following details:

- Controller: displays the attributes of the call controller that controls the port network as shown on the Monitoring Avaya Call Controllers page.
- IPSIs: displays the attributes of the IPSI boards on the port network as shown on the Monitoring IP Server Interface page.
- CLANs: displays the attributes of the CLANs associated with the port network as shown on the Monitoring CLAN page.

- MedPros: displays the attributes of the media processors associated with the port network as shown on the Monitoring Media Processors page.
- Total Load:displays the total load on the port network as shown on the Monitoring Total Load Metrics page.
- Intercom Load: displays the TDM time slot usage and the number of TDM time slots used (seizures) by intercom calls as shown on the Monitoring Intercom Load Metrics page.
- Incoming Trunk Load: displays the TDM time slot usage and the number of TDM time slots used (seizures) by incoming trunk calls as shown on the Monitoring Incoming Trunk Load Metrics page.
- Outgoing Trunk Load: This tab page displays the TDM time slot usage and the number of TDM time slots used (seizures) by outgoing trunk calls as shown on the Monitoring Outgoing Trunk Load Metrics page.
- Tandem Trunk Load: displays the TDM time slot usage and the number of TDM time slots used (seizures) by incoming and outgoing tandem trunk calls (calls between trunks) as shown on the Monitoring Tandem Trunk Load Metrics page.
- Incidents: displays the incidents generated based on the threshold values exceeded.

The left pane lists the general attributes of the port network as shown in the following table.

General Attributes of the Port Network

Attribute	Description
Number	Denotes the port network number.
IPSI A IP Address	Denotes the IP address of the IP Server Interface (IPSI) A board on the port network.
IPSI A Service State	Displays the service state of the IPSI A board.
IPSI B IP Address	Denotes the IP address of the IP Server Interface (IPSI) B board on the port network.
IPSI B Service State	Displays the service state of the IPSI B board.

Monitoring IP Server Interface

This tab page displays the attributes of the IPSI boards on the port network as shown in the following table.

IPSI Attributes

Attribute	Description
Fault State	Displays the Avaya G3 alarm status of the IPSI board. The possible values are: Warning, Minor, Major, and Clear.
Service State	Denotes the service state of the IPSI board. The service state can be one of the following: • In: denotes that the IPSI service is in the active state. • Out: denotes that the IPSI service is in the inactive state.
IP Address	Displays the IP address of the IPSI board.
Control State	Displays the control state of the IPSI board. The control state can be one of the following for the IPSI board: • Active: indicates that the control state for the IPSI board is in the active state. • Standby: indicates that the control state for the IPSI board is in the Standby state.

You can view the details of a IPSI in a form.

To view the IP Server Interface Details Form:

From the list of IPSIs listed on the tab page, select the IPSI of your interest, and then click . The IP Server Interface Details Form opens.

To view the Node Form for the IPSI, click , and then click **Open**. The Node Form opens displaying the details of the IPSI.

Analysis Pane

The Analysis pane displays a summary of the details of the selected IPSI as follows:

IP Server Interface Details Summary tab

- IP Address: The IP address of the selected IPSI board.
- Management Server: The management server for the IPSI board. This attribute displays one of the following values:
  - Local: If the IPSI board is being managed by the NNMi management server console on which you are viewing the IPSI board details.
  - Name of the regional manager that manages the IPSI board.

IP Server Interface Information tab

- Management Mode: The management status of the selected IPSI board.
- DHCP ID: The Dynamic Host Configuration Protocol (DHCP) ID of the IPSI board.

- Service State: The service state of the IPSI (In or Out).
- Control State: The control state of the IPSI (Active, Standby, or Unknown).

IP Server Interface Details Form

The IP Server Interface Details Form is split into two panes. The right pane displays the following details for the IPSI:

- Port Network: Displays the details of the port network on which the IPSI board is present as shown on the Monitoring Avaya Port Networks page. You can click the **Open** icon after selecting a port network to go to the Port Network Details Form.
- Incidents: Displays the incidents related to the IPSI.

The left pane displays the general attributes and the status of the IPSI as follows:

General Attributes of the IPSI

Attribute	Description
Hosted Node	The hostname of the IPSI board
Name	The name of the IPSI board.
IP Address	The IP address of the IPSI board.
Management Mode	Displays the management state of the IPSI. The status can be one of the following strings: • Managed: indicates that the IPSI is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the IPSI is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the IPSI is currently not managed by the NNM iSPI for IP Telephony.
Description	The description of the IPSI board.
DHCP ID	The DHCP ID of the IPSI board.
Location	The location of the IPSI board.
Vintage	The firmware vintage of the board.

Status of the IPSI

Attribute	Description
Service State	Displays the service state of the IPSI (In or Out).
Control State	Displays the control state of the IPSI (Active, Standby, or Unknown).
State of Health	Displays the state of health of the IPSI.

To view the Node Form for the IPSI, click , and then click **Open**. The Node Form opens displaying the details of the IPSI.

Monitoring CLAN

The CLAN tab page displays the attributes of the CLAN associated to the port network. The attributes are as follows:

Attribute	Description
Fault State	The Avaya G3 alarm status of the CLAN. The possible values are: Warning, Minor, Major, and Clear.
IP Address	The IP address of the CLAN.
Name	The name assigned to the CLAN.

To view the CLAN Details form:

From the CLAN tab page, select the CLAN of your interest, and then click . The CLAN Details Form opens.

Analysis Pane

The Analysis pane displays a summary of the details of the selected CLAN as follows:

CLAN Details Summary tab

- Name: The name assigned to the selected CLAN.
- Management Address: The external (public) IP address of the selected CLAN.
- Management Server: The management server for the CLAN. This attribute displays one of the following values:
  - Local: If the CLAN is being managed by the NNMi management server console on which you are viewing the CLAN details.
  - Name of the regional manager that manages the CLAN.

Avaya Control LAN Information tab

- Management Mode: The management status of the selected CLAN.
- IP Address: The internal (private) IP address of the selected CLAN.
- Location: The location of the selected CLAN board.
- Vintage: The firmware vintage for the selected CLAN.
- Description: The description of the selected CLAN.

CLAN Details Form

The CLAN Details Form is split into two panes. the right pane provides the following details:

- Socket Summary: displays the following details about the CLAN sockets usage

Note: In a GNM environment, the CLAN Details form on the global manager does not display the CLAN socket usage for port networks managed by regional managers.

Socket Detail	Description
Measurement Time	Lists the time at which the socket summary was collected.
Network Region	Displays the network region to which the CLAN is associated.
Management Mode	Displays the management state of the CLAN. The status can be one of the following strings: • Managed: indicates that the CLAN is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the CLAN is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the CLAN is currently not managed by the NNM iSPI for IP Telephony.
Usage	Lists the total time in Erlangs that is available from all the sockets on the CLAN.
Allocations	Lists the number of times a socket was allocated to a call or a link.
Allocation Denials	Lists the number of times sockets were unavailable to be allocated for calls or links.

Socket Detail	Description
Denial %	Lists the number of times sockets were unavailable to be allocated for calls or links in percentage. This percentage is obtained by dividing the Allocation Denials value from the sum of Usage and the Allocation Denials value.
Unavailability %	Lists the time in percentage during which the sockets were unavailable for use.
SNMP Access Error if Any	Displays if there were any SNMP access errors on the CLAN. The column displays None if there were no SNMP access errors.

- Port Network: displays the port network associated with the CLAN as shown on the Monitoring Avaya Port Networks page. You can select a port network that you want to view and click to see the Port Network Detail form for that port network.
- IP Phones: displays the IP phones associated with the CLAN as shown on the Monitoring Avaya IP Phones page. You can select an IP phone and click to view the Avaya IP Phones Details form for that phone.

The left pane displays the general attributes of the selected CLAN as follows.

Attribute	Description
Hosted Node	The hostname of the CLAN board.
Name	The name assigned to the CLAN board.
IP Address	The IP address of the CLAN board.
Location	The location of the CLAN board.
Vintage	The firmware vintage for the CLAN board.
Description	The description of the CLAN board.

To view the Node Form for the CLAN, click , and then click **Open**. The Node Form opens displaying the details of the CLAN.

Monitoring Media Processors

The MedPros tab page displays a list of media processors associated to the port network. The tab page displays the following attributes of the media processors.

Attributes of the Media Processors

Attribute	Description
Fault State	Displays the Avaya G3 alarm status of the media processor. The possible values are: Warning, Minor, Major, and Clear.
Control Link State	Displays the state of the media processor control link. The state can be any of the following: • Up: indicates that the link is up. • Down: indicates that the link is down.
Ethernet Link State	Displays the state of the media processor Ethernet link. The state can be any of the following: • Up: indicates that the link is up. • Down: indicates that the link is down.
IP Address	Displays the IP address for the media processor board.
Network Region	Displays the network region number that is associated with the media processor.
Name	Displays the name assigned to the media processor.

You can view the details of a single media processor in a form.

To view the Media Processor Details Form:

Select the media processor of your interest, and then click . The Media Processor Details Form opens.

Analysis Pane

The Analysis pane displays a summary of the details of the selected media processor as follows:

Media Processor Details Summary tab

- Name: The name of the selected media processor.
- Management Server: The management server for the media processor. This attribute displays one of the following values:
  - Local: If the media processor is being managed by the NNMi management server console on which you are viewing the media processor details.
  - Name of the regional manager that manages the media processor.

Avaya Media Processor Information tab

- Management Mode: The management status of the selected media processor.
- Description: The description of the media processor.

- IP Address: The IP address of the media processor.
- Location: The location of the media processor.
- Vintage: The firmware vintage of the media processor.
- MAC Address: The MAC address of the media processor.
- Network Region: The network region to which the media processor is associated.
- Alternate Network Region: The alternate network region to which the media processor is associated.
- Shared IP Address: The shared virtual IP address between the media processor and the duplicate media processor.
- Shared Virtual MAC: The shared virtual MAC address between the media processor and the duplicate media processor.

Avaya Media Processor State Information tab

- State: The state of the media processor. The state can be one of the following:
  - Active
  - Standby
  - Init
- IP Interface Enabled: Specifies if the IP Interface is enabled for the media processor board.
- Control Link State: Specifies the state of the media processor control link. The state can be Up or Down.
- Ethernet Link State: Specifies the state of the media processor Ethernet link. The state can be Up or Down.
- Peer Link State: Specifies the state of the media processor peer link state. The state can be Up or Down.
- DSP Channel Status 1: Specifies the service state of DSP resource 1. The status can be in-service or idle.
- DSP Channel Status 2: Specifies the service state of DSP resource 2. The status can be in-service or idle.
- DSP Channel Status 3: Specifies the service state of DSP resource 3. The status can be in-service or idle.
- DSP Channel Status 4: Specifies the service state of DSP resource 4. The status can be in-service or idle.

Media Processor Details Form

The Media Processor Details Form is split into two panes. The right pane displays the following details:

- Duplicated MedPro: displays the details of the duplicate media processor board associated as shown on the Monitoring Media Processors page. Click to open the Media Processor Detail form for the duplicate media processor board.
- Port Network: displays the details of the port network associated with the media processor as shown on the Monitoring Avaya Port Networks page. Click to open the Port Network Detail form.
- Incidents: displays the incidents relevant to the media processor.
- Network Regions: displays the network regions associated with the media processor as shown on the Monitoring Network Regions page. Click to open the IP Network Region Detail form for the network region.

The left pane lists the general attributes and the status of the media processor as follows.

General Attribute	Description
Hosted Node	The hostname of the media processor.
Name	The name of the media processor.
IP Address	The IP address of the media processor.
Management Mode	Displays the management state of the media processor. The status can be one of the following strings: • Managed: indicates that the media processor is managed by theNNM iSPI for IP Telephony. • Out of Service: indicates that the media processor is currently out of service and not managed by theNNM iSPI for IP Telephony. • Unmanaged: indicates that the media processor is currently not managed by theNNM iSPI for IP Telephony.
Description	The description of the media processor.
Location	The location of the media processor.
Vintage	The firmware vintage of the media processor.

General Attribute	Description
MAC Address	The MAC address of the media processor.
Network Region	The network region to which the media processor is associated.
Alt Network Region	The alternate network region to which the media processor is associated.
Shared IP Address	The shared virtual IP address between the media processor and the duplicate media processor.
Shared Virtual MAC	The shared virtual MAC address between the media processor and the duplicate media processor.

Status Attributes

Status Attribute	Description
State	The state of the media processor. The state can be one of the following: • Active • Standby • Init
IP Interface Enabled	Specifies if the IP Interface is enabled for the media processor board.
Control Link State	Specifies the state of the media processor control link. The state can be Up or Down.
Ethernet Link State	Specifies the state of the media processor Ethernet link. The state can be Up or Down.
Peer Link State	Specifies the state of the media processor peer link state. The state can be Up or Down.
DSP Channel Status 1	Specifies the service state of DSP resource 1. The status can be in-service or idle.
DSP Channel Status 2	Specifies the service state of DSP resource 2. The status can be in-service or idle.
DSP Channel Status 3	Specifies the service state of DSP resource 3. The status can be in-service or idle.
DSP Channel Status 4	Specifies the service state of DSP resource 4. The status can be in-service or idle.

To view the Node Form for the media processor, click , and then click **Open**. The Node Form opens displaying the details of the media processor.

Monitoring Port Network Load Details Metrics

The Port Network Details Form provides details of the load on the port network for the last hour. The load on the port network is calculated based on the following call type metrics:

- Intercom calls
- Trunk calls
  - Incoming trunk calls
  - Outgoing trunk calls
  - Tandem trunk calls (calls between trunks)

You can specify the threshold values for the metrics to identify the metric that violates the specified threshold. The Port Network Detail form provides the following tabs to view the load on the port network:

- Total Load: Lists the total load on the port network based on the Time Division Multiplexing (TDM) occupancy metric and the port network link occupancy metric. The metrics are displayed as percentage values as shown on the Monitoring Total Load page.
- Intercom Load: Lists the TDM time slot usage and the number of TDM time slots used (seizures) by calls within the same port network and calls made between different port networks as shown on the Monitoring Intercom Load page.
- Incoming Trunk Load: Lists the TDM time slot usage and the number of TDM time slot seizures by incoming trunk calls to stations within the same port network and incoming trunk calls from stations on different port networks as shown on the Monitoring Incoming Trunk Load page.
- Outgoing Trunk Load: Lists the TDM time slot usage and the number of TDM time slot seizures by outgoing trunk calls to stations within the same port network and outgoing trunk calls to stations on different port networks as shown on the Monitoring Outgoing Trunk Load page.
- Tandem Trunk Load: Lists the TDM time slot usage and the number of time slot seizures caused by incoming and outgoing tandem trunk calls (calls between two trunks) within the port network as shown on the Monitoring Tandem Trunk Load page.

Specifying Threshold Values for Metrics

You can specify the required threshold values for the metrics listed in the table to measure and monitor if the metric is within the threshold value you specified.

To specify a threshold value, do as follows:

1. Specify a threshold value for the required metric in the **Threshold Value** box for that metric.
2. Click **Save and Close** from the menu bar to apply the threshold value for the metric. After the next hour, the NNM iSPI for IP Telephony compares the metric with the specified value. If the value exceeds the specified threshold value, the NNM iSPI for IP Telephony generates an incident on the Incidents tab page of the Avaya Call Controller form.

Monitoring Total Load Metrics

This tab page displays the total load on the port network based on the following metrics collected for the last hour.

Metric	Description
TDM Occupancy (%)	The percentage of Time Division Multiplex (TDM) occupancy on the port network.
PN Link Occupancy (%)	The percentage of port network link occupancy on the port network.

Monitoring Intercom Load Metrics

This tab page displays the TDM time slot usage and the number of TDM time slots used (seizures) by calls within the same port network and calls made between different port networks. This page displays the following metrics collected for the last hour.

Metric	Description
Intra PN Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by calls in the same port network.
Intra PN Peg	The number of TDM time slot seizures by calls in the same port network.
Inter PN Usage (CCS)	The TDM time slot usage in CCS by calls between different port networks.
Inter PN Peg	The number of TDM time slot seizures by calls between different port networks.

Monitoring Incoming Trunk Load Metrics

This tab page displays the TDM time slot usage and the number of TDM time slots used (seizures) by incoming trunk calls within the same port network and incoming trunk calls to a port network from different port networks. This page displays the following metrics collected for the last hour.

Metric	Description
Intra PN Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by incoming trunk calls in the same port network.
Intra PN Peg	The number of TDM time slot seizures by incoming trunk calls in the same port network.
Incoming Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by incoming trunk calls from different port networks.
Incoming Peg	The number of TDM time slot seizures by incoming trunk calls from different port networks.
Outgoing Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by outgoing trunk calls to a port network in response to incoming trunk calls.
Outgoing Peg	The number of TDM time slot seizures by outgoing trunk calls to a port network in response to an incoming trunk calls.

Monitoring Outgoing Trunk Load Metrics

This tab page displays the TDM time slot usage and the number of TDM time slots used (seizures) by outgoing trunk calls within the same port network and outgoing trunk calls to different port networks. This page displays the following metrics collected for the last hour.

Metric	Description
Intra PN Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by outgoing trunk calls within the same port network.
Intra PN Peg	The number of TDM time slot seizures by outgoing trunk calls in the same port network.
Incoming Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by outgoing trunk calls from other port networks to this port network.
Incoming Peg	The number of TDM time slot seizures by outgoing trunk calls from other port networks to this port network.
Outgoing Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by outgoing trunk calls to other port networks.
Outgoing Peg	The number of TDM time slot seizures by outgoing trunk calls to other port networks.

Monitoring Tandem Trunk Load Metrics

This tab page displays the TDM time slot usage and the number of TDM time slots used (seizures) by incoming and outgoing tandem trunk calls (calls between trunks) within the same port network and between different port networks. This page displays the following metrics collected for the last hour.

Metric	Description
Intra PN Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by tandem trunk calls within the same port network.
Intra PN Peg	The number of TDM time slot seizures by tandem trunk calls in the same port network.
Incoming Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by incoming tandem trunk calls from other port networks.
Incoming Peg	The number of TDM time slot seizures by incoming tandem trunk calls from other port networks.
Outgoing Usage (CCS)	The TDM time slot usage in Centum Call Seconds (CCS) by outgoing tandem trunk calls to other port networks.
Outgoing Peg	The number of TDM time slot seizures by outgoing tandem trunk calls to other port networks.

Monitoring Avaya IP Phones

The IP Phones view displays a list of available Avaya IP phones in the network. The view arranges the key attributes of all discovered Avaya IP phones in a table.

To launch the Avaya IP Phones view, follow this step:

- From the **Workspaces** navigation pane, click **Avaya IP Telephony** > **IP Phones**. The IP Phones view opens in the right pane.

Basic Attributes of the IP Phones Table

Attribute	Description
Registration State	The registration status of the Avaya IP phone line with its current controller. Possible values are: ▪ Registered ▪ Unregistered

Basic Attributes of the IP Phones Table, continued

Attribute	Description
Active	Indicates the Avaya IP phones that are in active RTP sessions. **Note:** Make sure that the RTCP Reception for Avaya is configured in the Data Access Configuration form of the NNM iSPI for IP Telephony. **Note:** By default, auto-refresh of the table view is turned off. To refresh the table view, click (the **Refresh** icon).
Extension Number	The extension number of the IP phone.
Name	The name of the entity to which the phone is registered.
IP Address	The IP address of the phone.
Tenant	The name of the tenant to which the IP phone belongs.
Controller	The IP address of the call controller that controls the phone.
CLAN	The IP address of the Control LAN (CLAN) to which the phone is registered.
Management Server	The management server for the IP phone. This attribute displays one of the following values: ■ **Local**: If the IP phone is being managed by the NNMi management server console on which you are viewing the IP phone details. ■ Name of the regional manager that manages the IP phone.

When the status of a phone changes to *Unregistered*, the NNM iSPI for IP Telephony sends an incident to the NNMi incident browser.

You can view the details of a single IP phone in a form.

To view the Avaya IP Phone Details form:

In the IP Phones view, select the node of your interest, and then click . The Avaya IP Phone Details form opens.

To view the Node Form for the IP phone, click , and then click **Open**. The Node Form opens displaying the details of the IP phone.

Viewing Avaya IP Telephony Reports

You can select an IP phone from the inventory and click **Actions** > **IP Telephony Reports** and select one of the following options to launch a chart detail report for the selected attribute:

- Average Duration of Calls Made
- Average Duration of Calls Received
- Termination Reasons for Calls Made
- Termination Reasons for Calls Received.

See the NNM iSPI for IP Telephony Avaya IPT CDR Collection extension pack report online help for more information.

Analysis Pane

The Analysis pane of the IP Phone displays a summary of the details of the selected IP Phone as follows:

Avaya IP Phone Details Summary tab

- Name: The name of the selected IP phone.
- Controller: The call controller with which the selected IP phone is registered.
- Tenant: The name of the tenant to which the IP phone belongs.
- Management Server: The management server for the IP phone. This attribute displays one of the following values:
  - **Local**: If the IP phone is being managed by the NNMi management server console on which you are viewing the IP phone details.
  - Name of the regional manager that manages the IP phone.

General Information tab

- Management Mode: The management status of the selected IP phone.
- Registration State: The registration status of the selected IP phone line with its current call controller.
- Extension Number: The extension number of the IP phone.
- IP Address: The IP address of the selected IP phone.
- Service State: Indicates the service state of the IP phone.
- Model: The model of the selected IP phone.

Filtering Avaya IP phones

You can filter the listed IP phones in the Avaya IP Phones view with the available filters. You can perform the filtering action only on the **Registration State**, **Extension Number**, **IP Address**, **Tenant**, **Controller**, or the **Management Server** columns.

Note: You can select multiple filters based on your requirements.

To filter the Avaya IP Phones view, follow these steps:

1. Select an IP Phone, listed in the Avaya IP Phones view, and right-click one of the following column attributes:
   - **Registration State**
   - **Extension Number**
   - **IP Address**
   - **Tenant**
   - **Controller**
   - **Management Server**
2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the IP phones that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the IP Phones for which the selected column is not empty.
   - **Is empty**: filters and lists all the IP Phones for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the IP phones that do not have the value in the column that you selected.

The filtered list of IP phones appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Avaya IP Phones Details Form

The Avaya IP Phones Details form is split into two panes, the right pane and the left pane. The right pane lists the following details:

- Controller: This tab displays the attributes of the Call Controller with which the phone is associated as shown on the Monitoring Avaya Call Controllers page.
- CLAN: This tab displays the attributes of the CLAN with which the phone is registered as

displayed on the Monitoring CLAN page.

- Incidents: This tab displays the incidents related to the IP phone.

The left pane lists the following general attributes about the IP Phone:

Attribute	Description
Hosted Node	The hostname of the Avaya IP phone.
Extension Number	The extension number of IP phone.
IP Address	The IP address of the extension.
Management Mode	Displays the management state of the IP Phone. The status can be one of the following strings: • Managed: indicates that the IP Phone is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the IP Phone is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the IP Phone is currently not managed by the NNM iSPI for IP Telephony.
Registration State	The registration state of the IP phone line.
Name	The name of the IP phone.
Model	The model number of the IP phone.
Service State	Specifies the service state of the extension.
Busied for Maintenance	Specifies whether the station has been made busy for maintenance to be performed.
Call Forwarding Destination	The IP phone to which the calls are set to be forwarded from this extension.
Building	Displays the building location of the IP phone.
Floor	Displays the floor location of the IP phone.
Room	Displays the room location of the IP phone.
Phone Port	Displays the port used by the phone.
Location	The location configured for the IP phone.
Site-Code	The site code configured for the IP phone.
Mail-Code	The mail code configured for the IP phone.

The attribute displays **No Data** adjacent to the attributes that are not configured for the IP phone.

Analysis Pane

The Analysis pane displays a summary of the details of the selected IP phone. For more information, see Monitoring Avaya IP Phones.

Monitoring Media Gateways

The Media Gateways table displays a list of discovered Avaya media gateways on the network.

To launch the Media Gateways view, follow this step:

- From the **Workspaces** navigation pane, click **Avaya IP Telephony Media Gateways**. The Media Gateways view opens in the right pane. The table displays the following details about the discovered media gateways.

Basic Attributes of the Media Gateways Table

Attribute	Description
Registration State	The registration status of the media gateway with its current call controller. Possible values are: ▪ Registered ▪ Unregistered
Fault State	The Avaya G3 alarm status of the media gateway. The possible values are: Warning, Minor, Major, and Clear.
Name	The name of the media gateway.
IP Address	The IP address of the media gateway.
Tenant	The name of the tenant to which the media gateway belongs.
Network Region	The network region number associated with the media gateway.
Controller	The IP address of the call controller that controls the media gateway.
Hardware Type	The hardware type of the media gateway.
Management Server	The management server for the media gateway. This attribute displays one of the following values: ▪ **Local**: If the media gateway is being managed by the NNMi management server console on which you are viewing the media gateway details. ▪ Name of the regional manager that manages the media gateway.

You can view the details of a single media gateway in a form.

To view the Media Gateway Details form, follow this step:

- Select the media gateway of your interest, and then click . The Media Gateway Detailed form opens.

Analysis Pane

The Analysis pane of the Media Gateways displays a summary of the details of the selected media gateway as follows:

Media Gateways Details Summary tab

- Call Server: The IP address of the call server that controls the media gateway.
- Management Address: The external (public) IP address of the media gateway.
- Controller: The IP address of the call controller that controls the media gateway.
- Tenant: The name of the tenant to which the media gateway belongs.
- Management Server: The management server for the media gateway. This attribute displays one of the following values:
  - Local: If the media gateway is being managed by the NNMi management server console on which you are viewing the media gateway details.
  - Name of the regional manager that manages the media gateway.

Extension Information tab

- Management Mode: The management status of the selected media gateway.
- Network Region: The network region to which the media gateway is associated.
- Hosted Node: The hostname of the media gateway.
- Description: The description of the media gateway.
- Firmware Version: The firmware version of the media gateway.
- Network Region: The number of network regions to which the media gateway is associated.
- Registration State: The registration status of the media gateway with its current call controller.
- H.248 Link State: The state of the H.248 link.
- H.248 Link Error: Indicates if there were any errors on the H.248 link.
- Number of Media Modules: The number media modules associated with the selected media gateway.
- Number of VoIP Engines: The number VoIP engines associated with the selected media gateway.

- Number of DSP Cores: The number DSP cores associated with the selected media gateway.
- Faults: Indicates the faults generated for the selected media gateway.

Filtering Avaya Media Gateways

You can filter the listed media gateways in the Media Gateways view based on the following attributes:

- Registration State
- Name
- IP Address
- Tenant
- Network Region
- Controller
- Hardware Type
- Management Server

Note: You can create filters for each of the listed attributes to view only the required media gateways.

To filter the Media Gateways view:

1. Right-click any of the listed attribute columns of one of the media gateways listed in the Media Gateways view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the media gateways that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the media gateways for which the selected column is not empty.
   - **Is empty**: filters and lists all the media gateways for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the media gateways that do not have the value in the column that you selected.

The filtered list of media gateways appears in the view.

You can also filter the media gateways by right clicking the attribute column headings and selecting **Filter** and one of the following options:

- Is not empty
- Is empty
- Create Filter

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Media Gateway Details Form

The Media Gateway Detailed form is split into two panes. The right pane lists the following details:

- VOIP Settings: displays the VOIP settings for the gateway as shown on the VOIP Settings tab page.
- Clock Settings: displays the clock settings for the gateway as shown on the Clock Settings tab page.
- Media Modules: displays the details specific to the media modules associated with the media gateway as shown on the Monitoring Media Modules page.
- VOIP Engines: displays the details specific to the VOIP engines associated with the media gateway as shown on the Monitoring VOIP Engines page.
- DSP Cores: displays the details specific to the DSP cores associated with the media gateway as shown on the Monitoring DSP Cores page.
- Network Regions: displays the details specific to the network regions associated with the media gateway as shown on the Monitoring Network Regions page.
- Incidents: displays the incidents specific to the media gateway.

The left pane displays the general attributes, states, and faults for the media gateway as shown in the following tables.

General Attributes of the Media Gateway

Attribute	Description
Hosted Node	The hostname of the media gateway.
Name	The name of the media gateway.

General Attributes of the Media Gateway, continued

Attribute	Description
IP Address	The IP address of the media gateway.
Management Mode	Displays the management state of the media gateway. The status can be one of the following strings: • Managed: indicates that the media gateway is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the media gateway is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the media gateway is currently not managed by the NNM iSPI for IP Telephony.
Hardware Type	The hardware type of the media gateway.
Serial Number	The serial number of the media gateway.
Hardware Vintage	The hardware version of the media gateway.
Vintage Suffix	The vintage suffix of the media gateway.
Network Region	The network region to which the media gateway is associated.
Description	The description of the media gateway.
Default IP Address	The default IP address for the media gateway.
Gateway Number	The gateway number configured for the media gateway.
MAC Address	The MAC address of the media gateway.
Firmware Version	The firmware version of the media gateway.
Controller List	The controller list for the media gateway.
DHCP for IP Address	Indicates if DHCP is configured for the IP address.
DHCP for VLAN	Indicates if DHCP is configured for the VLAN.
DHCP for Controllers	Indicates if DHCP is configured for the call controllers.

General Attributes of the Media Gateway, continued

Attribute	Description
DHCP for VOIP Engine	Indicates if DHCP is configured for the VOIP engine.
DHCP Site Specific Option	Indicates the DHCP site-specific option set.

State Attributes for Media Gateway

Attribute	Description
Controller	The IP address of the call controller to which the media gateway is registered.
Registration State	The registration state of the media gateway.
H.248 Link State	The state of the H.248 link.
H.248 Link Error	Indicates if there were any errors on the H.248 link.

The **Faults** section lists the faults generated for the media gateway.

To view the Node Form for the media gateway, click , and then click **Open**. The Node Form opens displaying the details of the media gateway.

Monitoring Media Modules

The Media Modules tab page displays the details specific to the media modules associated with the media gateway. This page displays the following details.

Attributes of the Media Modules

Attribute	Description
Faults Active	Specifies if this feature is enabled on the media module.
Name	The name of the media module.
Number	The number assigned to uniquely identify the media module.
Type	The type of the media module.

You can view the details of a single media module in a form.

To view the Media Modules form, follow this step:

- Select the media module of your interest, and then click . The Media Modules form opens.

Filtering Avaya Media Modules

You can filter the listed media modules in the Media Modules tab page based on the following attributes:

- Faults Active
- Name
- Number
- Type

Note: You can create filters for each of the listed attributes to view only the required media modules.

To filter the Media Modules tab page view:

1. Right-click any of the listed attribute columns of one of the media modules listed in the Media Modules tab page view and select **Filter**.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the media modules that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the media modules for which the selected column is not empty.
   - **Is empty**: filters and lists all the media modules for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the media modules that do not have the value in the column that you selected.

     The filtered list of media modules appears in the view.

   You can also filter the media modules by right clicking the attribute column headings and selecting **Filter** and one of the following options:

   - Is not empty
   - Is empty
   - Create Filter

All the attributes that you can use to filter are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to use to filter.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Media Modules Form

The Media Modules form is split into two panes. The right pane lists the incidents generated for the media module. The left pane displays the general attributes and the state of the media module as shown in the following table.

General Attributes of the Media Module

Attribute	Description
Name	The name of the media module.
Management Mode	Displays the management state of the media module. The status can be one of the following strings: • Managed: indicates that the media module is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the media module is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the media module is currently not managed by the NNM iSPI for IP Telephony.
Description	The description of the media module.
Number	The number assigned to uniquely identify the media module.
Serial Number	The serial number of the media module.
Hardware Vintage	The hardware vintage number of the media module.
Vintage Suffix	The vintage suffix of the media module.
Firmware Version	The firmware version of the media module.
Number of Ports	The number of ports on the media module.
Number of Channels.	The number of channels on the media module.

The **Faults** section displays the faults associated with the media module.

Monitoring VOIP Engines

The VOIP Engines tab page displays the details specific to the VOIP engines associated with the media gateway. This page displays the following details.

Attributes of the VOIP Engines

Attribute	Description
Administrative State	Indicates the administrative state of the VOIP engine.
Faults Active	Specifies if this feature is enabled on the VOIP engine.
DSP State	Specifies the Digital Signal Processor (DSP) state on the VOIP engine.
ID	Lists the ID of the VOIP engine.
IP Address	Lists the IP address of the VOIP engine.

You can view the details of a single VOIP engine in a form.

To view the VOIP Engines form:

Select the VOIP engine of your interest, and then click . The VOIP Engines form opens.

Filtering Avaya VOIP Engines

You can filter the listed VOIP engines in the VOIP Engines tab page based on the following attributes:

- Administrative State
- Faults Active
- DSP State
- ID
- IP Address

Note: You can create filters for each of the listed attributes to view only the required VOIP engines.

To filter the VOIP Engines tab page view:

1. Right-click any of the listed attribute columns of one of the VOIP engines listed in the VOIP Engines tab page view and select **Filter**.

2. Select one of the following filters:
   - **Equals this value**: filters and lists all the VOIP engines that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the VOIP engines for which the selected column is not empty.
   - **Is empty**: filters and lists all the VOIP engines for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the VOIP engines that do not have the value in the column that you selected.

     The filtered list of VOIP engines appears in the view.

   You can also filter the VOIP engines by right clicking the attribute column headings and selecting **Filter** and one of the following options:

   - Is not empty
   - Is empty
   - Create Filter

   All the attributes, except for the **Administrative State**, are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to use to filter.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

VOIP Engines Form

The VOIP Engines form is split into two panes. The right pane lists the following details:

- DSP Cores: displays the details of the DSP cores associated with the VOIP engine as shown on the Monitoring DSP Cores page,
- Incidents: displays the incidents related to the VOIP engine.

The left pane displays the general attributes and state of the VOIP engine as shown in the following table.

General Attributes of the VOIP Engine

Attribute	Description
IP Address	The IP address of the VOIP engine.

General Attributes of the VOIP Engine, continued

Attribute	Description
Management Mode	Displays the management state of the VOIP engine. The status can be one of the following strings: • Managed: indicates that the VOIP engine is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the VOIP engine is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the VOIP engine is currently not managed by the NNM iSPI for IP Telephony.
MAC Address	The MAC address of the VOIP engine.
ID	The unique ID of the VOIP engine.
Default IP Address	The default IP address assigned to the VOIP engine.
Firmware Version	The firmware version of the VOIP engine.
Total Channels	The total number of channels on the VOIP engine.

State Attributes of the VOIP Engine

Attribute	Description
Administrative State	The administrative state of the VOIP engine.
DSP State	The DSP state of the VOIP engine.
Channels in Use	The number of channels in use on the VOIP engine.
Jitter Buffer Size	The buffer size allocated to jitter on the VOIP engine.
Hyperactivity Detected	Specifies whether hyperactivity is detected on the VOIP engine.
5-Minute Average Occupancy	Specifies the value for this parameter specified on the VOIP engine.

The **Faults** section lists the faults generated for the VOIP engine.

Monitoring DSP Cores

The DSP Cores tab page displays the details of the DSP cores associated with the media gateway. This page displays the following details.

Attributes of the DSP Cores

Attribute	Description
Administrative State	The administrative state of the DSP core.
DSP State	The state of the DSP core. the state can be one of the following: • In Use • Idle
DSP Core ID	The unique identification number for the DSP core.
VOIP Engine ID	The ID of the VOIP Engine associated with the DSP core.

You can view the details of a single DSP core in a form.

To view the DSP Cores form:

Select the DSP core of your interest, and then click . The DSP Cores form opens.

Filtering Avaya DSP Cores

You can filter the listed DSP cores in the DSP Cores tab page based on the following attributes:

- Administrative State
- DSP State
- DSP Core ID
- VOIP Engine ID

Note: You can create filters for each of the listed attributes to view only the required DSP cores.

To filter the DSP Cores tab page view:

1. Right-click any of the listed attribute columns of one of the DSP cores listed in the DSP Cores tab page view and select **Filter**.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the DSP cores that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the DSP cores for which the selected column is not empty.

- **Is empty**: filters and lists all the DSP cores for which the selected column is empty.
- **Not equal to this value**: filters and lists all the DSP cores that do not have the value in the column that you selected.

  The filtered list of DSP cores appears in the view.

You can also filter the DSP cores by right clicking the attribute column headings and selecting **Filter** and one of the following options:

- Is not empty
- Is empty
- Create Filter

All the attributes, except for the **Administrative State**, are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to use to filter.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

DSP Cores Form

The DSP Cores form displays the general attributes and the states of the DSP core as shown in the following table.

General Attributes of DSP Core

Attribute	Description
DSP Core ID	The unique identifier for the DSP core.
Management Mode	Displays the management state of the DSP core. The status can be one of the following strings: • Managed: indicates that the DSP core is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the DSP core is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the DSP core is currently not managed by the NNM iSPI for IP Telephony.
VOIP Engine IP Address	The IP address of the VOIP engine associated with the DSP core.

General Attributes of DSP Core, continued

Attribute	Description
VOIP Engine ID	The unique identifier of the VOIP engine associated with the DSP core.
Total Channels	The total number of channels on the DSP core.
Channels in Use	The total number of channels in use on the DSP core.

State Attributes of DSP Core

Attribute	Description
Administrative State	The administrative state of the DSP core.
DSP State	The DSP state of the DSP core.

Cisco IP Telephony

The Cisco IP Telephony workspace enables you to view the inventory views for the Cisco devices and entities that are discovered and monitored in your environment. The following table lists the options that you can click to view the details of a discovered device or an entity:

Inventory View	Purpose
UCM Clusters	Lists the Cisco Unified Communications Manager (CUCM) Clusters discovered on the network.
UCMEs	Lists the Cisco Unified Call Manager Expresses (UCMEs) discovered on the network.
IP Phones	Lists the Cisco IP Phones discovered on the network.
Gatekeepers	Lists the Cisco Gatekeepers discovered on the network.
Unity Devices	Lists the Cisco Unity Devices discovered on the network.

Monitoring Cisco Unified Communications Manager Clusters

The UCM Clusters view displays the details of the Cisco Unified Communications Manager clusters discovered on the network. The view arranges the key attributes of all the discovered UCM clusters in a table.

To launch the UCM Clusters view, follow this step:

- From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.

Basic Attributes of the Clusters Table

Attribute	Description
Name	Indicates the name of the UCM cluster discovered.
Custom Info	Indicates the custom information configured for the cluster. This attribute displays *Not Set* if you have not specified the custom information for the cluster.
Tenant	Indicates the name of the tenant to which the UCM cluster belongs.
Management Server	The management server for the cluster. This attribute displays one of the following values: • **Local**: If the cluster is being managed by the NNMi management server console on which you are viewing the cluster details. • Name of the regional manager that manages the cluster.

You can view the details of a single cluster using the UCM Cluster Details form.

To view the Cisco Cluster Details form, follow this step:

- In the UCM Clusters view, select the cluster of your interest, and then click . The UCM Cluster Details form opens.

Analysis Pane

The Analysis pane displays a summary of the details of the selected UCM cluster as follows:

UCM Cluster Details Summary tab

- Name: The name of the selected UCM cluster.
- Tenant: The name of the tenant to which the UCM cluster belongs.
- Management Server: The management server for the cluster. This attribute displays one of the following values:
  - **Local**: If the cluster is being managed by the NNMi management server console on which you are viewing the cluster details.
  - Name of the regional manager that manages the cluster.

General Information tab

- UCM Subscriber Groups: the names of the UCM subscriber groups in the selected UCM cluster.
- Number of UCMs: The number of UCMs associated with the selected UCM cluster.

- Number of Device Pools: The number of device pools associated with the selected UCM cluster.
- Number of H.323 Gateways: The number of H.323 gateways associated with the selected UCM cluster.
- Number of MGCP/SCCP Gateways: The number of MGCP/SCCP gateways associated with the selected UCM cluster.
- Number of Extensions: The number of IP phones associated with the selected UCM cluster.
- Number of SRSTs: The number of SRSTs associated with the selected UCM cluster.
- Number of H323 Trunks: The number of H323 trunks associated with the selected UCM cluster.
- Number of SIP Trunks: The number of SIP trunks associated with the selected UCM cluster.
- Number of Media Devices: The number of media devices associated with the selected UCM cluster.
- Number of Locations: The number of locations associated with the selected UCM cluster.
- NTP Server: The comma separated list of the NTP Servers associated with the selected UCM cluster.
- Custom Info: The custom information configured for the UCM cluster.

Based on the configurations to monitor the state of additional attributes that indicate the health, performance, and availability of the Cisco Unified Communications Manager clusters and Cisco Unified Communications Managers, their components, and associated devices, the following tabs are displayed:

- **UCM Call Activity tab**

Displays the details of the measurement attributes configured for the UCM Call Activity. For more information about the measurement attributes configured for UCM Call Activity, see Monitoring Call Activities.

- **Registered Devices Count tab**

Displays the details of the measurement attributes configured for the Registered Devices Count. For more information about the measurement attributes configured for Registered Devices Count, see Monitoring Registered Devices Count.

- **Gateway Call Activity tab**

Displays the details of the measurement attributes configured for the Gateway Call Activity. For more information about the measurement attributes configured for Gateway Call Activity, see Monitoring Gateway Call Activity.

- **Configurations tab**

Displays the details of the measurement attributes configured for the route lists and hunt lists in the cluster. For more information about the measurement attributes configured for the route lists and hunt lists in the cluster, see Monitoring Route List and Hunt List Count.

- **Media Resource Activity tab**

Displays the details of the measurement attributes configured for the Media Resource Activity. For more information about the measurement attributes configured for Media Resource Activity, see Monitoring Media Resource Activity.

- **CTIManager Connections Count tab**

Displays the details of the measurement attributes configured for the CTIManager Connections Count. For more information about the measurement attributes configured for CTIManager Connections Count, see Monitoring CTIManager Connections Count.

- **Locations tab**

Displays the details of the measurement attributes configured for the Cisco Locations. For more information about the measurement attributes configured for Locations, see Monitoring Locations.

- **SIP Trunk Sessions tab**

Displays the details of the measurement attributes configured for the SIP Trunk Sessions. For more information about the measurement attributes configured for SIP Trunk Sessions, see Monitoring SIP Trunk Sessions.

Filtering UCM Clusters

You can filter the listed Unified Call Manager (UCM) clusters in the UCM Clusters view with the available filters. You can perform the filtering action on the **Name**, **Custom Info**, **Management Server**, or **Tenant** columns.

Note: You can select multiple filters based on your requirements.

To filter the UCM Clusters view, follow these steps:

1. Right-click the **Name**, **Custom Info**, **Management Server** or **Tenant** attribute of one of the UCM clusters listed in the UCM Clusters view.

2. Select one of the following filters:

   - **Equals this value**: filters and lists all the UCM clusters that have a value that is equal to the value of the column that you selected.

- **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
- **Is not empty**: filters and lists all the UCM clusters for which the selected column is not empty.
- **Is empty**: filters and lists all the UCM clusters for which the selected column is empty.
- **Not equal to this value**: filters and lists all the UCM clusters that do not have the value in the column that you selected.

The filtered list of UCM clusters appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

UCM Cluster Details Form

The Unified Communications Manager (UCM) Cluster Details form is split into two panes. The left pane displays the following general attributes of the selected UCM cluster:

- UCM Cluster Name
- Number of UCM Subscriber Groups
- Number of Associated Device Pools
- Custom Info: You can type the custom information required for the cluster and click (the **Save** icon) to save the custom information for the cluster.

The right pane displays the following tabs:

- UCM Subscriber Groups
- UCMs
- Device Pools
- H.323 Gateways
- MGCP/SCCP Gateways
- IP Phones
- SRST Routers
- H323 Trunks

- SIP Trunks
- NTP Servers
- Media Devices
- Voice Mail Devices
- Locations

Analysis Pane

The Analysis pane displays a summary of the details of the selected UCM cluster. For more information, see Monitoring UCM Clusters.

Monitoring UCM Subscriber Groups

The UCM Subscriber Group view displays the details of the UCM subscriber groups (call manager groups) associated with a UCM cluster. The view arranges the key attributes of all UCM subscriber groups in a table.

To launch the UCM Subscriber Groups view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click Open. The UCM Cluster Details form opens.
3. Click the UCM Subscriber Groups tab. The UCM Subscriber Groups view opens on the right pane.

Basic Attributes of the UCM Subscriber Group Table

Attribute	Description
Name	Indicates the name of UCM subscriber group.
Custom Info	The custom information configured for the UCM subscriber group. This attribute displays *Not Set* if you have not specified the custom information for the UCM subscriber group.

Select a UCM Subscriber Group from the list of UCM Subscriber Groups displayed and click Open to open the UCM Subscriber Group Details form. This form displays the attributes for the selected UCM Subscriber Group.

Filtering UCM Subscriber Groups

You can filter the listed UCM Subscriber Groups in the UCM Subscriber Groups view with the available filters. You can perform the filtering action on the **Name**, or **Custom Info** columns.

Note: You can select multiple filters based on your requirements.

To filter the UCM Subscriber Groups view:

1. Right-click the **Name**, or **Custom Info** attribute of one of the UCM subscriber groups listed in the UCM Subscriber Groups view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the UCM subscriber groups that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the UCM subscriber groups for which the selected column is not empty.
   - **Is empty**: filters and lists all the UCM subscriber groups for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the UCM subscriber groups that do not have the value in the column that you selected.

The filtered list of UCM subscriber groups appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

The Analysis pane provides a summary of the details of a selected UCM subscriber group as follows:

UCM Subscriber Group Details Summary tab

- Name: The name of the selected UCM subscriber group.
- Cluster: The name of the UCM cluster to which the selected UCM subscriber group is associated.
- Management Server: The management server for the UCM subscriber group. This attribute displays one of the following values:
  - Local: If the UCM subscriber group is being managed by the NNMi management server console on which you are viewing the UCM subscriber group details.
  - Name of the regional manager that manages the UCM subscriber group.

General Information tab

- Primary Call Manager: The name of the primary call manager of the selected UCM subscriber group.
- Number of Device Pools: The number of device pools associated with the selected UCM subscriber group.
- Custom Info: The custom information configured for the selected UCM subscriber group.

Registered Devices Count tab

This tab provides the count of the following registered devices in the UCM subscriber group:

- Hardware Phones
- Other IP Phones
- MGCP/SCCP Gateway Endpoints
- MGCP/SCCP FXO Ports
- MGCP/SCCP FXS Ports
- MGCP/SCCP E&M Ports
- MGCP/SCCP T1/E1 PRI Ports
- MGCP/SCCP T1/E1 CAS Ports
- Analog Access Gateway Boxes
- H.323 Gateway Boxes
- Media Resources
- CTI Ports
- CTI Route Points
- VM Ports
- Other Station Devices[1]

Note: You may not be able to see the counts of the registered devices if you have not enabled monitoring of the devices. For more information, see Configure Registered Devices Count Monitoring.

[1]The counts of the Soft IP Phones, VM Ports, CTI Route Points, and CTI Ports are summed up to calculate the count of Other Station Devices.

UCM Subscriber Group Details Form

The UCM Subscriber Group details form is split into two panes. The right pane (UCM Subscribers) displays the details of the UCM subscribers associated with the UCM Subscriber Group as listed in the Monitoring UCMs page.

The left pane lists the general attributes and the priority of the UCMs within the UCM Subscriber Group as listed in the following tables.

General

General Attribute	Description
UCM Subscriber Group Name	Indicates the name of the UCM Subscriber Group.
Number of UCM Subscribers	Indicates the number of associated UCM Subscribers in the UCM Subscriber Group.
Number of Associated Device Pools	Indicates the number of device pools in the UCM Subscriber Group.
Custom Info	Displays the custom information configured for the UCM Subscriber Group. You can type the custom information required for the UCM Subscriber Group and click (Save) to save the custom information for the UCM Subscriber Group.

UCM Subscribers

This section lists the primary, secondary, and tertiary subscribers configured in the UCM Subscriber group.

You can select a Cisco Unified Communications Manager subscriber from the **UCM Subscribers** tab page and click (Open) to open the Cisco Call Controller Details form and view the details of the specific UCM subscriber.

Analysis Pane

The Analysis pane displays a summary of the details of the selected UCM subscriber group. For more information, see Monitoring UCM Subscriber Groups.

Monitoring Cisco Unified Communications Managers

The UCMs view displays all Cisco Unified Communications Managers associated with a UCM cluster. The view arranges the key attributes of all the discovered UCMs in a table.

To launch the UCMs view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click (Open). The UCM Cluster Details form opens.
3. Click the UCMs tab. The UCMs view opens on the right pane.

Basic Attributes of the Cisco Call Controllers Table

Attribute	Description
CallManager Service State	The state of the CallManager Service running in the UCM. The possible values are: • Up • Down • Unknown • Not Monitored
Name	The name configured for the UCM.
IP Address/Hostname	The IP address or the hostname of the UCM.
Version	The version of the UCM.
UCM Cluster	The name of the cluster to which the UCM is associated.
Roles	The roles of the UCM. The possible values are as follows: • Publisher: The UCM with this role holds all the configuration data for the cluster. • Subscriber: The UCM with this role handles the call processing. • Publisher, Subscriber: The UCM that performs both the publisher and subscriber roles. **Note:** To discover all the devices associated with a device pool in a cluster, you must configure the AXL configuration details for the UCM with the publisher role. You can perform this configuration using the **AXL Access** tab in the Data Access Configuration form.

Filtering UCMs

You can filter the listed UCMs in the UCMs view based on the management server.

To filter the UCMs view, follow these steps:

1. Right-click the **Management Server** attribute column of one of the UCMs listed in the UCMs view.

2. Select one of the following filters:
   - **Equals this value**: filters and lists all the UCMs that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the UCMs for which the selected column is not empty.
   - **Is empty**: filters and lists all the UCMs for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the UCMs that do not have the value in the column that you selected.

     The filtered list of UCMs appears in the view.

   Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

You can view the details of a single UCM in a form.

To view the Call Controller form, follow this step:

- From the UCMs view, select the UCM of your interest, and then click (Open). The Call Controller Details form opens.

To view the Node Form for the Call Controller server, click , and then click **Open**. The Node Form opens displaying the details of the Call Controller server.

Analysis Pane

The Analysis pane provides a summary of the details of a selected UCM as follows:

Cisco Call Controller Details Summary tab

- Name: The name of the selected UCM.
- Cluster: The name of the UCM cluster to which the selected UCM is associated.
- Management Server: The management server for the UCM. This attribute displays one of the following values:
  - Local: If the UCM is being managed by the NNMi management server console on which you are viewing the UCM details.
  - Name of the regional manager that manages the UCM.

General Information tab

- Management Mode: The management status of the selected UCM.
- IP Address: The IP address of the selected UCM.
- Controller Type: The type of the selected UCM. For UCMs, the only possible value in this field is Cisco Call Manager.
- Version: The version of the selected UCM.
- Description: A short description of the selected UCM.
- Role: The role of the selected UCM.
- UCM Subscriber Groups (CM Priority): The names of the UCM subscriber groups to which the selected UCM is associated.

Availability tab

This tab provides the information about the availability of UCM administrative console.You may not be able to get this information if you have not enabled monitoring of the administration web page. For more information, see Enabling the Monitoring of the Call Manager Administration Web Page State.

Cisco Tftp Server tab

This tab provides the information about the activities related to the configuration file builds performed by the Cisco TFTP server. To see these details, you must enable monitoring of the Cisco TFTP Server activities. For more information, see Enabling the Monitoring of the Cisco TFTP Server.

Registered Devices Count tab

This tab provides the counts of the registered devices that are monitored in the UCM. You may not be able to see the counts of the registered devices if you have not enabled monitoring of the devices. For more information, see Enabling the Monitoring of Registered Devices Count.

Services tab

This tab provides the information about the availability of Unified Communications Operating System (UCOS) services.You may not be able to see these details if you have not enabled monitoring of these services. For more information, see Enabling the Monitoring of the Availability of Services on the UCM.

System Health tab

This tab provides the information about the system health parameters.You may not be able to see the parameters if you have not enabled monitoring of the system health parameters. For more information, see Enabling the Monitoring of System Health Parameters.

UCM Call Activity tab

This tab provides the counts of the call activities on the UCM. To see these details, you must enable monitoring of the call activities for the UCM. For more information, see Enabling the Monitoring of UCM Call Activity.

Cisco Call Controller Details Form

If you select a Unified Communication Manager (UCM), Survivable Remote Site Telephony (SRST) router, or Unified Call Manager Express (UCME) and click the Open icon, you can see the details of the selected UCM, UCME, or SRST router in the Cisco Call Controller Details form.

The Cisco Call Controller Details form helps you view the node details of the selected Cisco Call Controller server, the associated gatekeepers, the IP phones associated with it, and the IP phones configured with an SRST router. The form presents two different panes.

The right pane lists the following details:

- Gatekeepers: The Gatekeepers tab displays the details of all the gatekeepers associated with the selected Cisco Call Controller server. The tab displays the details of every associated gatekeeper in the format presented in the Cisco Gatekeepers view.
- Controlled IP Phones: The Controlled IP Phones tab displays the details of all the IP phones associated with the selected Cisco Call Controller server. The tab displays the details of every associated IP phone in the format presented in the Cisco IP Phones view.
- *Only visible when launched from the SRST Routers tab.* Configured IP Phones: The Configured IP Phones tab displays the list of IP phones configured with an SRST router. The tab displays the details of the IP phones registered with the SRST Router as shown in the SRST Router Configured IP Phones page.
- Incidents: The incidents generated for the Cisco Unified Communications Manager state changes.

The left pane lists the following details of the selected Cisco Unified Communications Manager.

Basic Attributes

Attribute	Description
Hosted Node	The node on which the Call Controller is hosted.
Name	The name of the Cisco Unified Communications Manager or SRST router.
IP Address	The IP address of the Call Controller server.

Basic Attributes, continued

Attribute	Description
Management Mode	The management status of the node. The status can be any of the following strings: • Managed: indicates that the node is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the node is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the NNM iSPI for IP Telephony.
Type	The type of the Cisco Call Controller. The type can be one of the following: • Cisco Call Manager • Cisco Call Manager Express • SRST Router
Version	The version of the server.
Description	A short description of the server.

Call Manager Specific Attributes

Attribute	Description
UCM Cluster	Specifies the name of the Cisco Unified Communications Manager cluster.
CallManager Service State	The CallManager Service State of the selected Cisco Call Controller server. This attribute is not applicable for UCMEs. The possible values for a UCM are: • Up—indicates the selected UCM is UP • Down—indicates the selected UCM is DOWN • Unknown—indicates the SNMP response, which indicates the state of the UCM, is not available from the node. • Not Monitored—indicates the selected UCM is not currently monitored.

Only visible when launched from the SRST Router view. SRST Router Specific Attributes

Attribute	Description
E Phone Communication IP	The IP address of the SRST router interface that the E Phones use to communicate during a fallback.
SCCP Communication Port	The SCCP port that the phones use to communicate.
Max Conferences	The maximum number of conferences that can run simultaneously.
Max Directory Numbers	The maximum number of directory numbers that can be configured on the device.
Max E Phones	The maximum number of Ethernet phones (E phones) that can be registered with the device.
Voice Mail Number	The voicemail number configured for the device.
Total SCCP IP Phones Registered	The total number of SCCP IP Phones registered with the device.
Total SIP Phones Registered	The total number of SIP phones registered with the device.
State	The state of an SRST Router can be one of the following: • Active—indicates that the SRST router is in the active state and is the current call controller for the IP phones registered with the SRST Router. The SRST router state changes to active when the primary Call Controller for the registered phones is not available. • Standby—indicates that the SRST router is in the standby state and is not the current Call Controller for the IP Phones registered with the SRST Router. • Unknown—indicates the SNMP response, which indicates the state of the SRST router, is not available from the node. • Not Monitored—indicates the selected SRST router is not currently monitored.

Only visible when launched from the UCMEs view. **Call Manager Express Attributes**

Attribute	Description
EPhone Communication IP	The communication IP address used by the EPhone to communicate with the Call Manager Express.
SCCP Communication Port	The SCCP communication port used by EPhones to communicate with the Call Manager Express.
Max Conferences	The maximum number of conferences that can run simultaneously on the device.
Max Directory Numbers	The maximum number of directory numbers that you can configure with the device.
Max E Phones	The maximum number of E Phones that you can configure with the device.
Voice Mail Number	The voicemail number configured for the device.
Total SCCP IP Phones Registered	The total number of SCCP IP Phones registered with the Call Manager.

Analysis Pane

The Analysis pane provides a summary of the details of a selected Cisco Call Controller as follows:

Cisco Call Controller Details Summary tab

- Name: The name of the selected Cisco Call Controller.
- Management Address *(Only when launched from the UCMs view)*: The external (public) IP address of the selected UCM.
- Cluster *(Only when launched from the UCMs or SRST Routers view)*: The name of the cluster to which the UCM or SRST router belongs.
- Device Pool (Only when launched from the SRST Routers view): The name of the device pool with which the SRST router is associated.
- Tenant (Only when launched from the UCMEs view): The name of the tenant to which the UCME belongs.
- Management Server: The management server for the Cisco Call Controller. This attribute displays one of the following values:
  - Local: If the Cisco Call Controller is being managed by the NNMi management server console on which you are viewing the Cisco Call Controller details.
  - Name of the regional manager that manages Cisco Call Controller.

General Information tab

- Management Mode: The management status of the selected Cisco Call Controller.
- IP Address: The IP address of the selected Cisco Call Controller.
- Controller Type: The type of the selected Cisco Call Controller.
- Version: The version of the selected Cisco Call Controller.
- Description: A short description of the selected Cisco Call Controller.

Only when launched from the UCMEs or SRST Routers view. **Device Registrations tab**

- Registered IP Phones: The number of IP phones associated with the selected SRST router or Cisco Unified Communications Manager Express.
- Configured IP Phones: The number of IP phones configured with the SRST router.

Monitoring Device Pools

The Device Pools view displays all device pools associated with a UCM cluster. The view arranges the names of all device pools in a table.

To discover and monitor device pools, you must configure the AXL access for the Cisco Unified Communications Manager publisher server of the cluster to which the device pools are registered.

To launch the Device Pools view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click (Open). The UCM Cluster Details form opens.
3. Click the Device Pools tab. The Device Pools view opens on the right pane.

Filtering Device Pools

You can filter the listed device pools in the Device Pools view based on Device Pool Name.

To filter the Device Pools view, follow these steps:

1. Right-click the **Device Pool Name** attribute column of one of the device pools listed in the Device Pools view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the device pools that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.

- **Is not empty**: filters and lists all the device pools for which the selected column is not empty.
- **Is empty**: filters and lists all the device pools for which the selected column is empty.
- **Not equal to this value**: filters and lists all the device pools that do not have the value in the column that you selected.

  The filtered list of device pools appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

You can view the details of a single device pool in a form.

To view the Device Pool Details form, follow this step:

- From the Device Pools view, select the device pool of your interest, and then click (Open). The Device Pool Details form opens.

Analysis Pane

The Analysis pane of the device pool displays a summary of the details of the selected device pool as follows:

Device Pool Details Summary tab

- Device Pool Name: The name of the selected device pool.
- UCM Cluster: The name of the UCM cluster to which the selected device pool is associated.
- Management Server: The management server for the device pool. This attribute displays one of the following values:
  - Local: If the device pool is being managed by the NNMi management server console on which you are viewing the device pool details.
  - Name of the regional manager that manages the device pool.

Device Pool Information tab

- UCM Subscriber Group: The name of the UCM subscriber group to which the selected device pool is associated.
- Number of IP Phones: The number of IP phones associated with the selected device pool.
- Number of MGCP/SCCP Gateways: The number of MGCP/SCCP gateways associated with the selected device pool.

- Number of H.323 Gateways: The number of H.323 gateways associated with the selected device pool.
- Number of SRSTs: The number of SRST routers associated with the selected device pool.
- Number of IC Trunks: The number of IC trunks associated with the selected device pool.
- Number of Media Devices: The number of media devices associated with the selected device pool.

Registered Devices Count tab

This tab provides the count of the following registered devices in the device pool:

- Hardware Phones
- Other IP Phones
- MGCP/SCCP Gateway Endpoints
- MGCP/SCCP FXO Ports
- MGCP/SCCP FXS Ports
- MGCP/SCCP E&M Ports
- MGCP/SCCP T1/E1 PRI Ports
- MGCP/SCCP T1/E1 CAS Ports
- Analog Access Gateway Boxes
- H.323 Gateway Boxes
- Media Resources
- CTI Ports
- CTI Route Points
- VM Ports
- Other Station Devices[1]

Note: You may not be able to see the counts of the registered devices if you have not enabled monitoring of the devices. For more information, see Configure Registered Devices Count Monitoring.

[1]The counts of the Soft IP Phones, VM Ports, CTI Route Points, and CTI Ports are summed up to calculate the count of Other Station Devices.

Device Pool Details Form

The Device Pool Details form helps you view the IP phones, Media Gateway Control Protocol (MGCP) gateways, Skinny Call Control Protocol (SCCP) gateways, H.323 gateways, SRST routers, IC trunks, and media devices associated with the selected device pool.

To launch the Device Pool Details view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click (Open). The UCM Cluster Details form opens.
3. Click the **Device Pools** tab, select a device pool of your interest, and then click (Open). The Device Pool Details form opens.

The form presents the details of a device pool in two panes, the left pane and the right pane. The left pane displays the general attributes of the selected device pool.

General Attributes

Attribute	Description
Cluster Name	Indicates the name of Unified Communications Manager (UCM) Cluster to which the selected device pool is associated.
CM Group Name	Indicates the name of Call Manager (CM) group to which the selected device pool is associated.
Primary CM Name	Indicates the name of the primary call manager of the CM group.
Secondary CM Name	Indicates the name of the secondary call manager of the CM group.
Tertiary CM Name	Indicates the name of the tertiary call manager of the CM group.

The right pane of device pool details form displays the following tabs:

- **IP Phones**: Displays the IP phones associated with the device pool. You can filter the listed IP phones using the available filtering options. If you select an IP phone, you can see the summary of the selected IP phone in the Analysis pane. For more information, see Monitoring IP Phones.
- **MGCP/SCCP Gateways**: Displays all the Media Gateway Control Protocol (MGCP) and Skinny Call Control Protocol (SCCP) gateways associated with the device pool. You can filter the listed gateways using the available filtering options. If you select an MGCP/SCCP gateway, you can see the summary of the selected gateway in the Analysis pane. For more information, see Monitoring MGCP/SCCP Gateways.

- **H.323 Gateways**: Displays all the H.323 gateways associated with the device pool. The view arranges the key attributes of all the discovered H.323 gateways in a table. You can filter the listed H.323 gateways using the available filtering options. If you select an H.323 gateway, you can see the summary of the selected H.323 gateway in the Analysis pane. For more information, see Monitoring H.323 Gateways.
- **SRST Routers** : Displays the Survivable Remote Site Telephony (SRST) routers associated with the device pool. The view arranges the key attributes of all associated SRST routers in a table. If you select an SRST router, you can see the summary of the selected SRST router in the Analysis pane. For more information, see SRST Routers.
- **H323 Trunks**: Displays the intercluster trunks (IC trunks) associated with the device pool. The view arranges the key attributes of all associated IC trunks in a table. If you select an IC trunk, you can see the summary of the selected IC trunk in the Analysis pane. For more information, see Monitoring H323 Trunks.
- **Media Devices**: Displays all media devices associated with the device pool. The view displays all types of media devices like Media Termination Point (MTP) devices, conference bridges, transcode devices, annunciators, and so on. If you select a media device, you can see the summary of the selected media device in the Analysis pane. For more information, see Monitoring Media Devices.

Analysis Pane

The Analysis pane displays a summary of the details of the selected device pool. For more information, see Monitoring Device Pools.

Monitoring H.323 Gateways

The H.323 Gateways view displays all the H.323 gateways associated with a UCM cluster. The view arranges the key attributes of all H.323 gateways in a table.

To launch the H.323 Gateways view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click (Open). The UCM Cluster Details form opens.
3. Click the H.323 Gateways tab. The H.323 Gateways view opens on the right pane.

Basic Attributes of the Cisco Voice Gateway Table

Attribute	Description
Operational State	The status of the H.323 gateway device. Possible values are: • NOT_ MONITORED • NOT_ POLLED • UNKNOWN • NORMAL • WARNING • MINOR • CRITICAL
IP Address	The IP address of the H.323 gateway device.
Protocol	The protocol used by the H.323 device.
UCM Cluster	The name of the UCM cluster to which the H.323 gateway belongs.
Device Pool	The name of the device pool to which the H.323 gateway is associated. **Note:** To see the association with the device pool, you must configure AXL credentials for the cluster to which the device pool is associated. See the section Configuring Data Access for Cisco for more details.
Call Server	The fully-qualified domain name of the UCM device to which the H.323 gateway device is configured.
Custom Info	Indicates the custom information configured for the H.323 gateway.
Description	A description of the H.323 gateway device.

Filtering H.323 Gateways

You can filter the listed H.323 gateways in the H.323 Gateways view based on the following attributes:

- Operational State
- IP Address
- Protocol
- UCM Cluster

- Device Pool
- Call Server
- Custom Info

Note: You can create filters for each of the listed attributes to view only the required H.323 gateways.

To filter the H.323 Gateways view:

1. Right-click any of the listed attribute columns of one of the H.323 gateways listed in the H.323 Gateways view and select **Filter**.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the H.323 gateways that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the H.323 gateways for which the selected column is not empty.
   - **Is empty**: filters and lists all the H.323 gateways for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the H.323 gateways that do not have the value in the column that you selected.

     The filtered list of H.323 gateways appears in the view.

   You can also filter the H.323 gateways by right clicking the attribute column headings and selecting **Filter** and one of the following options:

   - Is not empty
   - Is empty
   - Create Filter

All the attributes that you can use to filter are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to use to filter.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

The Analysis pane provides a summary of the details of a selected H.323 gateway as follows:

Voice Gateway Summary tab

- Cluster: The names of the UCM clusters to which the selected H.323 gateway is associated.
- Device Pool: The names of the device pools to which the selected H.323 gateway is associated.
- Call Server: The fully-qualified domain names of the UCM devices with which the selected H.323 gateway device is configured.
- Management Server: The management server for the H.323 gateway. This attribute displays one of the following values:
  - Local: If the H.323 gateway is being managed by the NNMi management server console on which you are viewing the H.323 gateway details.
  - Name of the regional manager that manages the H.323 gateway.

General Information tab

- Management Mode: The management status of the selected H.323 gateway device.
- IP Address: The IP address of the selected H.323 gateway device.
- Operational State: The status of the selected H.323 gateway device.
- Model: The model of the selected H.323 gateway.
- Protocol: The protocol configured for the selected H.323 gateway.
- Description: The description configured for the selected H.323 gateway.

Gateway Call Activity tab

This tab provides the information about the active calls and the current active calls handled by the gateway. For an H.323 gateway associated with more than one cluster, the values of the configured measurement types for each of the cluster, to which the user has access, is displayed. Each measurement type displays the names of the clusters, in parentheses, associated to the H.323 gateway. To see these details, you must enable the monitoring of gateway call activity. For more information, see Enabling the Monitoring of Gateway Call Activity.

Voice Gateway Interface Details tab

- Number of Digital T1 CAS Interfaces: The number of digital T1 CAS interfaces in the selected H.323 gateway.
- Number of ISDN T1 PRI Interfaces: The number of ISDN T1 PRI interfaces in the selected H.323 gateway.
- Number of Digital E1 CAS Interfaces: The number of digital E1 CAS interfaces in the selected H.323 gateway.

- Number of ISDN E1 PRI Interfaces: The number of ISDN E1 PRI interfaces in the selected H.323 gateway.
- Number of Other Interfaces: The number of other interfaces in the selected H.323 gateway.

Viewing Cisco Voice Gateway Details Form

You can launch the Voice Gateway details view to view the details of a Voice Gateway device.

To launch the Voice Gateway details view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click Open. The UCM Cluster Details form opens.
3. Click the **H.323 Gateways** tab, select a device pool of your interest, and then click Open. The Voice Gateway details form opens.

The details form for a Voice Gateway device includes an additional tab—the **Voice Gateway Interfaces** tab. The Voice Gateway Interfaces tab arranges all the key attributes of all the interfaces of the Gateway device in a table.

The form lists the general attributes of the voice gateway as shown in the following table.

Attribute	Description
Hosted Node	Indicates the node for the gateway. Click Open to see the details of the node.
Name	Indicates the name of the gateway.
IP Address	Indicates the IP address for the gateway.
Model	Indicates the model of the gateway.
Gateway Version	Indicates the version of the gateway.
Protocol	Indicates the protocol configured for the gateway.
Description	Indicates the description configured for the gateway.
Operational State	Indicates the operational state of the gateway.
Custom Info	Indicates the custom information configured for the gateway.

Attribute	Description
Management Mode	Displays the management state of the gateway. The status can be one of the following strings: • Managed: indicates that the node is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the node is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the NNM iSPI for IP Telephony.

Analysis Pane

The Analysis pane displays a summary of the details of the selected voice gateway. For more information, see Monitoring H.323 Gateways.

Monitoring MGCP/SCCP Gateways

The MGCP/SCCP Gateways view displays all the Media Gateway Control Protocol (MGCP) gateways, and Skinny Call Control Protocol (SCCP) gateways associated with a UCM cluster. The view arranges the key attributes of all the discovered MGCP and SCCP gateways in a table.

To launch the MGCP/SCCP Gateways view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click (Open). The UCM Cluster Details form opens.
3. Click the MGCP/SCCP Gateways tab. The MGCP/SCCP Gateways view opens on the right pane.

Basic Attributes of the Cisco Voice Gateway Table

Attribute	Description
Registration State	Indicates if the MGCP/SCCP gateway is registered with a UCM. The possible values are as follows: • Unknown • Registered • Unregistered • Rejected • Partially Registered
Name	The hostname of the MGCP/SCCP gateway.
Type	The type of the MGCP/SCCP gateway. Possible values are: • E and M port • FXS port • ISDN T1 PRI
CCM Device Name	The name of the MGCP/SCCP gateway.
UCM Cluster	The name of the UCM cluster to which the MGCP/SCCP gateway belongs.
Device Pool	The name of the device pool to which the MGCP/SCCP gateway is associated. **Note:** To see the association with the device pool, you must configure AXL credentials for the cluster to which the device pool is associated. See the section Configuring Data Access for Cisco for more details.

Basic Attributes of the Cisco Voice Gateway Table, continued

Attribute	Description
Usage State	The usage status of the MGCP/SCCP gateway. This state is not applicable for non-DS1 gateways. Possible values are: • idle— if all channels associated with the gateway are idle. • in use—if all channels associated with the gateway are in use. • partially in use—if at least one channel is in use (not all the channels are in use). • not polled—if the gateway is not polled. • not applicable—if the usage state is not applicable for the gateway. • unknown—if the usage state is not known.
Operational State	This field indicates the operational state of the gateway. Possible values are: • Up • Down • Testing • Unknown • Dormant • Not Present • Lower Layer Down
Custom Info	Indicates the custom information configured for the MGCP/SCCP gateway.

Filtering MGCP/SCCP Gateways

You can filter the listed MGCP/SCCP gateways in the MGCP/SCCP Gateways view based on the following attributes:

- Registration State
- Name
- Type
- CCM Device Name
- UCM Cluster

- Device Pool
- Usage State
- Operational State
- Custom Info

Note: You can create filters for each of the listed attributes to view only the required MGCP/SCCP gateways.

To filter the MGCP/SCCP Gateways view:

1. Right-click any of the listed attribute columns of one of the MGCP/SCCP gateways listed in the MGCP/SCCP Gateways view and select **Filter**.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the MGCP/SCCP gateways that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the MGCP/SCCP gateways for which the selected column is not empty.
   - **Is empty**: filters and lists all the MGCP/SCCP gateways for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the MGCP/SCCP gateways that do not have the value in the column that you selected.

   The filtered list of MGCP/SCCP gateways appears in the view.

   You can also filter the MGCP/SCCP gateways by right clicking the attribute column headings and selecting **Filter** and one of the following options:

   - Is not empty
   - Is empty
   - Create Filter

All the attributes that you can use to filter are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to use to filter.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

The Analysis pane provides a summary of the details of a selected MGCP/SCCP gateway as follows:

Voice Gateway Interfaces Summary tab

- Name: The name of the selected MGCP/SCCP gateway.
- Call Server: The fully-qualified domain name of the UCM device to which the selected MGCP/SCCP gateway device is configured.
- Cluster: The name of the UCM cluster to which the selected MGCP/SCCP gateway is associated
- Management Server: The management server for the MGCP/SCCP gateway. This attribute displays one of the following values:
  - Local: If the MGCP/SCCP gateway is being managed by the NNMi management server console on which you are viewing the MGCP/SCCP gateway details.
  - Name of the regional manager that manages the MGCP/SCCP gateway.

Cisco VGW Interface Information tab

- Type: : The type of the MGCP/SCCP gateway.
- Registration State: Indicates if the MGCP/SCCP gateway is registered with a UCM.
- Usage State: The usage status of the MGCP/SCCP gateway.
- Operational State: the operational state of the selected MGCP/SCCP gateway.
- Total Number of Channels: The number of channels in the selected MGCP/SCCP gateway.
- Total Number of B-Channels: The number of B-Channels in the selected MGCP/SCCP gateway.

Gateway Call Activity tab

This tab provides the information about the active calls handled by the MGCP/SCCP gateway. To see these details, you must enable monitoring of gateway call activity. For more information, see Enabling the Monitoring of Gateway Call Activity.

Voice Gateway Interface Details Form

The Gateway Interface details form helps you view the details of the selected gateway interface. The left pane of a gateway interface details form displays the general attributes of the interface. The right pane displays the key attributes of the gateway channels in the selected gateway interface.

Node Form: Voice Gateway Interfaces Tab

The Voice Gateway Interfaces tab lists the key attributes of the endpoints of the Cisco Voice Gateway device.

Basic Attributes of the Voice Gateway Interfaces Tab

Attribute	Description
Registration State	Indicates if the endpoint is registered with a Cisco CallManager. This state is applicable only for interfaces with the Media Gateway Control Protocol (MGCP). Possible values are: • Unknown • Registered • Unregistered • Rejected • Partially Registered
Name	The hostname of the endpoint.
Type	The type of the endpoint. Possible values are: • E and M port • FXS port • ISDN T1 PRI
CCM Device Name	The name of the interface.
UCM Cluster	The name of the UCM cluster to which the endpoint belongs.
Device Pool	The name of the device pool to which the endpoint is associated.
Usage State	The usage status of the endpoint. This state is not applicable for non-DS1 interfaces. Possible values are: • Idle— if all channels associated with the interface are idle. • In-use—if all channels associated with the interface are in use. • Partially in-use—if at least one interface is in use (not all the interfaces are in use).
Custom Info	Indicates the custom information configured for the voice gateway interface.

Attribute	Description
Operational State	This field indicates the operational state of the endpoint. Possible values are: • Up • Down • Testing • Unknown • Dormant • Not Present • Lower Layer Down

General Attributes of the Voice Gateway Interfaces

Attribute	Description
NNMi Interface	The name of the associated NNMi interface.
Name	The name for the voice gateway interface.
CCM Device Name	The name of the Cisco Call Manager (CCM) device configured for the voice gateway interface.
Type	The type of the voice gateway interface.
Model	The model of the voice gateway interface.
Speed	The speed of the voice gateway interface.
Description	The description configured for the voice gateway interface.
Registration State	The registration state of the voice gateway interface.
Usage State	The usage state of the voice gateway interface.
Operational State	The operational state of the voice gateway interface.
Device Pool	The name of the device pool to which the gateway interface is associated.
Custom Info	The custom information configured for the voice gateway interface.

Analysis Pane

The Analysis pane provides a summary of the details of a selected gateway interface as follows:

Voice Gateway Interfaces Summary tab

- Name: The name of the selected gateway interface.
- Call Server: The fully-qualified domain name of the UCM device to which the selected gateway interface is configured.
- Cluster: The name of the UCM cluster with which the selected gateway interface is associated.
- Management Server: The management server for the gateway interface. This attribute displays one of the following values:
  - Local: If the gateway interface is being managed by the NNMi management server console on which you are viewing the gateway interface details.
  - Name of the regional manager that manages the gateway interface.

Cisco VGW Interface Information tab

- Type: The type of the gateway interface.
- Registration State: Indicates if the gateway interface is registered with a UCM.
- Usage State: The usage status of the gateway interface.
- Operational State: the operational state of the selected gateway interface.
- Total Number of Channels: The number of channels in the selected gateway interface.
- Total Number of B-Channels: The number of B-Channels in the selected gateway interface.

Gateway Call Activity tab

Applicable only for MGCP/SCCP gateway interfaces. This tab provides the information about the active calls handled by the gateway interface. To see these details, you must enable monitoring of gateway call activity. For more information, see Configure Gateway Call Activity Monitoring. The H.323 gateway interfaces display the value as *Not Applicable*.

Voice Gateway Channels Details Form

The Voice Gateway Channels details form displays the general attributes of the selected voice gateway channel.

Basic Attributes of the Voice Gateway Channels Tab

Attribute	Description
NNMi Interface	The name of the associated NNMi interface.
Name	The name of the channel.
Type	The type of the channel.

Basic Attributes of the Voice Gateway Channels Tab, continued

Attribute	Description
Usage State	The usage state of the channel. Possible values are: • In-use • Idle • Unknown • Not-polled

Analysis Pane

The Analysis pane provides a summary of the details of a selected gateway channel as follows:

Voice Gateway Channels Summary tab

- Name: The name of the selected channel.
- Management Server: The management server for the gateway channel. This attribute displays one of the following values:
  - Local: If the gateway channel is being managed by the NNMi management server console on which you are viewing the gateway channel details.
  - Name of the regional manager that manages the gateway channel.

Cisco VGW Channel Information tab

- Type: The type of the channel.
- Usage State: The usage state of the channel.

Monitoring SRST Routers

The SRST Routers view displays the details of the Survivable Remote Site Telephony (SRST) routers associated with a UCM cluster. The view arranges the key attributes of the SRST routers in a table.

To discover and monitor SRST nodes, you must configure the AXL access for the Cisco Unified Communications Manager publisher server of the cluster to which the SRST nodes are registered.

To launch the SRST Routers view, follow these steps:

1. From the **Workspaces** pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.

2. Select a UCM Cluster of your interest and click (Open). The UCM Cluster Details form opens.

3. Click the **SRST Routers** tab. The SRST Routers view opens on the right pane.

Basic Attributes of the SRST Routers Table

Attribute	Description
State	The State of the SRST router. The possible values are: • Active • Standby • Unknown • Not Monitored
Name	The hostname of the SRST router.
IP Address	The IP address of the SRST router.
Version	The version of the SRST router.
UCM Cluster	The name of the UCM cluster to which the SRST router belongs.
Device Pool	The name of the device pool to which the SRST router is associated. **Note:** To see the association with the device pool, you must configure AXL credentials for the cluster to which the device pool is associated. See the section Configuring Data Access for Cisco for more details.

Filtering SRST Routers

You can filter the listed SRST router in the SRST Routers view based on the management server.

To filter the SRST Routers view:

1. Right-click the **Management Server** attribute column of one of the SRST routers listed in the SRST Routers view.

2. Select one of the following filters:
   - **Equals this value**: filters and lists all the SRST routers that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.

- **Is not empty**: filters and lists all the SRST routers for which the selected column is not empty.
- **Is empty**: filters and lists all the SRST routers for which the selected column is empty.
- **Not equal to this value**: filters and lists all the SRST routers that do not have the value in the column that you selected.

  The filtered list of SRST routers appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

You can view the details of a single SRST router in a form.

To view the Call Controller form:

Select an SRST router from the list of SRST routers displayed and click (Open) to open the Call Controller Details Form. This form displays the attributes for the selected SRST router.

Analysis Pane

The Analysis pane provides a summary of the details of a selected SRST router as follows:

Cisco Call Controller Details Summary tab

- Cluster: The name of the UCM cluster to which the selected SRST router is associated.
- Device Pool: The name of the device pool to which the selected SRST router is associated.
- Management Server: The management server for the SRST router. This attribute displays one of the following values:
  - Local: If the SRST router is being managed by the NNMi management server console on which you are viewing the SRST router details.
  - Name of the regional manager that manages the SRST router.

General Information tab

- Name: The hostname of the SRST router. If the hostname is not available, the IP address is displayed.
- Management Mode: The management status of the selected SRST router device.
- Controller Type: The type of the selected SRST router. For SRST routers, the only possible value in this field is SRST Router.
- Version: The version of the selected SRST router.
- Description: A short description of the selected SRST router.

Device Registrations tab

- Registered IP Phone Extensions: The number of IP phones associated with the selected SRST router.
- Configured IP Phone Extensions: The number of IP phones managed by the selected SRST router.

Cisco Call Controller Details Form

If you select a Unified Communication Manager (UCM), Survivable Remote Site Telephony (SRST) router, or Unified Call Manager Express (UCME) and click the Open icon, you can see the details of the selected UCM, UCME, or SRST router in the Cisco Call Controller Details form.

The Cisco Call Controller Details form helps you view the node details of the selected Cisco Call Controller server, the associated gatekeepers, the IP phones associated with it, and the IP phones configured with an SRST router. The form presents two different panes.

The right pane lists the following details:

- Gatekeepers: The Gatekeepers tab displays the details of all the gatekeepers associated with the selected Cisco Call Controller server. The tab displays the details of every associated gatekeeper in the format presented in the Cisco Gatekeepers view.
- Controlled IP Phones: The Controlled IP Phones tab displays the details of all the IP phones associated with the selected Cisco Call Controller server. The tab displays the details of every associated IP phone in the format presented in the Cisco IP Phones view.
- *Only visible when launched from the SRST Routers tab.* Configured IP Phones: The Configured IP Phones tab displays the list of IP phones configured with an SRST router. The tab displays the details of the IP phones registered with the SRST Router as shown in the SRST Router Configured IP Phones page.
- Incidents: The incidents generated for the Cisco Unified Communications Manager state changes.

The left pane lists the following details of the selected Cisco Unified Communications Manager.

Basic Attributes

Attribute	Description
Hosted Node	The node on which the Call Controller is hosted.
Name	The name of the Cisco Unified Communications Manager or SRST router.
IP Address	The IP address of the Call Controller server.

Basic Attributes, continued

Attribute	Description
Management Mode	The management status of the node. The status can be any of the following strings: • Managed: indicates that the node is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the node is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the NNM iSPI for IP Telephony.
Type	The type of the Cisco Call Controller. The type can be one of the following: • Cisco Call Manager • Cisco Call Manager Express • SRST Router
Version	The version of the server.
Description	A short description of the server.

Call Manager Specific Attributes

Attribute	Description
UCM Cluster	Specifies the name of the Cisco Unified Communications Manager cluster.
CallManager Service State	The CallManager Service State of the selected Cisco Call Controller server. This attribute is not applicable for UCMEs. The possible values for a UCM are: • Up—indicates the selected UCM is UP • Down—indicates the selected UCM is DOWN • Unknown—indicates the SNMP response, which indicates the state of the UCM, is not available from the node. • Not Monitored—indicates the selected UCM is not currently monitored.

Only visible when launched from the SRST Router view. SRST Router Specific Attributes

Attribute	Description
E Phone Communication IP	The IP address of the SRST router interface that the E Phones use to communicate during a fallback.
SCCP Communication Port	The SCCP port that the phones use to communicate.
Max Conferences	The maximum number of conferences that can run simultaneously.
Max Directory Numbers	The maximum number of directory numbers that can be configured on the device.
Max E Phones	The maximum number of Ethernet phones (E phones) that can be registered with the device.
Voice Mail Number	The voicemail number configured for the device.
Total SCCP IP Phones Registered	The total number of SCCP IP Phones registered with the device.
Total SIP Phones Registered	The total number of SIP phones registered with the device.
State	The state of an SRST Router can be one of the following: • Active—indicates that the SRST router is in the active state and is the current call controller for the IP phones registered with the SRST Router. The SRST router state changes to active when the primary Call Controller for the registered phones is not available. • Standby—indicates that the SRST router is in the standby state and is not the current Call Controller for the IP Phones registered with the SRST Router. • Unknown—indicates the SNMP response, which indicates the state of the SRST router, is not available from the node. • Not Monitored—indicates the selected SRST router is not currently monitored.

Only visible when launched from the UCMEs view. **Call Manager Express Attributes**

Attribute	Description
EPhone Communication IP	The communication IP address used by the EPhone to communicate with the Call Manager Express.
SCCP Communication Port	The SCCP communication port used by EPhones to communicate with the Call Manager Express.
Max Conferences	The maximum number of conferences that can run simultaneously on the device.
Max Directory Numbers	The maximum number of directory numbers that you can configure with the device.
Max E Phones	The maximum number of E Phones that you can configure with the device.
Voice Mail Number	The voicemail number configured for the device.
Total SCCP IP Phones Registered	The total number of SCCP IP Phones registered with the Call Manager.

Analysis Pane

The Analysis pane provides a summary of the details of a selected Cisco Call Controller as follows:

Cisco Call Controller Details Summary tab

- Name: The name of the selected Cisco Call Controller.
- Management Address *(Only when launched from the UCMs view)*: The external (public) IP address of the selected UCM.
- Cluster *(Only when launched from the UCMs or SRST Routers view)*: The name of the cluster to which the UCM or SRST router belongs.
- Device Pool (Only when launched from the SRST Routers view): The name of the device pool with which the SRST router is associated.
- Tenant (Only when launched from the UCMEs view): The name of the tenant to which the UCME belongs.
- Management Server: The management server for the Cisco Call Controller. This attribute displays one of the following values:
  - Local: If the Cisco Call Controller is being managed by the NNMi management server console on which you are viewing the Cisco Call Controller details.
  - Name of the regional manager that manages Cisco Call Controller.

General Information tab

- Management Mode: The management status of the selected Cisco Call Controller.
- IP Address: The IP address of the selected Cisco Call Controller.
- Controller Type: The type of the selected Cisco Call Controller.
- Version: The version of the selected Cisco Call Controller.
- Description: A short description of the selected Cisco Call Controller.

Only when launched from the UCMEs or SRST Routers view. **Device Registrations tab**

- Registered IP Phones: The number of IP phones associated with the selected SRST router or Cisco Unified Communications Manager Express.
- Configured IP Phones: The number of IP phones configured with the SRST router.

Monitoring H323 Trunks

The H323 Trunks view displays the H323 intercluster trunks (IC trunks) associated with a UCM cluster. The view arranges the key attributes of all the associated H323 IC trunks in a table.

To launch the Cisco H323 Trunks view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click (Open). The UCM Cluster Details form opens.
3. Click the H323 Trunks tab. The H323 Trunks view opens on the right pane.

Basic Attributes of the IC Trunks Table

Attribute	Description
Registration State	The registration state of the intercluster trunk. Possible values are: • Registered • Unregistered • Rejected • Unknown • Not Applicable (for non-gatekeeper-controlled intercluster trunks)
Name	The name of the Cisco H323 trunk.

Basic Attributes of the IC Trunks Table, continued

Attribute	Description
UCM Cluster	The name of the UCM cluster to which the H323 trunk belongs.
UCM	The name of the Cisco Unified Communications Manager with which the H323 trunk is associated.
Type	The type of the H323 trunk. This field indicates if the H323 trunk is controlled by the gatekeeper or not.
Active Gatekeeper	The IP address of the gatekeeper device that controls the H323 trunk. If the H323 trunk is not controlled by a gatekeeper, the field remains blank.
Remote CM List	The list of Cisco CallManager servers that are connected to the H323 trunk (for non-gatekeeper-controlled intercluster trunk).
Device Pool	The name of the device pool to which the intercluster trunk is associated. **Note:** To see the association with the device pool, you must configure AXL credentials for the cluster to which the device pool is associated. For more information, see Configuring the NNM iSPI for IP Telephony to Access the AXL Data.

The NNM iSPI for IP Telephony retrieves the registration state of only gatekeeper-controlled H323 trunks. When the state of an intercluster trunk becomes *Rejected* or *Unregistered*, the NNM iSPI for IP Telephony sends an incident to the NNMi incident browser.

Filtering Cisco IC Trunks

You can filter the listed H323 trunks in the H323 Trunks view based on the following attributes of the H323 trunk:

- Registration State
- Name
- Type
- Active Gatekeeper
- Remote CM List
- Cluster
- Device Pool

Note: You can create filters for each of the listed attributes to view only the required IC trunks.

To filter the H323 Trunks view, follow these steps:

1. Right-click any of the listed attribute columns of one of the H323 trunks listed in the H323 Trunks view.

2. Select one of the following filters:
   - **Equals this value**: filters and lists all the H323 trunks that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the H323 trunks for which the selected column is not empty.
   - **Is empty**: filters and lists all the H323 trunks for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the H323 trunks that do not have the value in the column that you selected.

     The filtered list of H323 trunks appears in the view.

You can also filter the H323 trunks by right clicking the attribute column headings and selecting **Filter** and one of the following options:

- Is not empty
- Is empty
- Create Filter

Note: Apart from the **Registration State** attribute, all the other attributes that you can use to filter are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to use to filter.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

You can view the details of a single Cisco H323 trunk within a form.

To view the H323 Trunk form, follow :

In the H323 Trunks view, select the node of your interest, and then click (Open). The H323 Trunk Details Form opens.

To view the Node Form for the intercluster trunk, click , and then click **Open**. The Node Form opens displaying the details of the H323 trunk.

Analysis Pane

The Analysis pane provides a summary of the details of a selected H323 trunk as follows:

H323 Trunk Details Summary tab

- Name: The name of the selected the H323 trunk.
- Cluster: The name of the UCM cluster to which the selected the H323 trunk is associated.
- Device Pool: The name of the device pool to which the selected the H323 trunk is associated.
- Management Server: The management server for the H323 trunk. This attribute displays one of the following values:
  - Local: If the H323 trunk is being managed by the NNMi management server console on which you are viewing the H323 trunk details.
  - Name of the regional manager that manages the H323 trunk.

General Information tab

- Type: The type of the H323 trunk. This field indicates if the H323 trunk is controlled by the gatekeeper or not.
- Active GateKeeper: The IP address of the gatekeeper device that is active.
- Configured GateKeeper: The IP address of the gatekeeper device that controls the H323 trunk.
- Remote CM List: The list of UCMs that are connected to the H323 trunk (for non-gatekeeper-controlled H323 trunk).

H323 Trunk Details Form

The H323 Trunk form helps you view the node details of the selected H323 trunk and the gatekeepers associated with the trunk. The form presents two different panes.

The right pane lists the following details:

- Controlling gatekeepers: The Controlling Gatekeepers tab displays the details of the gatekeeper device that controls the intercluster trunk. The tab displays the details of the gatekeeper in the format presented in the Cisco Gatekeepers view.
- Incidents: This tab lists the incidents generated based on the state of the H323 trunk.

The left pane lists the following details of the selected Cisco H323 trunk:

Basic Attributes of the Selected Cisco H323 Trunk

Attribute	Description
Name	The name of the H323 trunk.
Type	Type of the Cisco H323 trunk.
Remote CM List	The list of Cisco CallManager servers that are connected to the H323 trunk.
UCM Cluster	The name of the UCM cluster to which the H323 trunk belongs.

Basic Attributes of the Gatekeeper

Attribute	Description
Configured	The IP address of the gatekeeper device that controls the H323 trunk.
Alternate	Lists the alternate gatekeeper devices configured to control the H323 trunk.
Active	The IP address of the gatekeeper device that is active.

Analysis Pane

The Analysis pane displays a summary of the details of the selected intercluster trunk. For more information, see Monitoring H323 Trunks.

Monitoring SIP Trunks

The SIP Trunks view displays the SIP trunks associated with a UCM cluster. The view arranges the key attributes of all associated SIP trunks in a table.

To launch the Cisco SIP Trunks view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest, and then click (the **Open** icon). The UCM Cluster Details form opens.
3. Click the SIP Trunks tab. The SIP Trunks view opens on the right pane.

Basic Attributes of the SIP Trunks Table

Attribute	Description
Name	Indicates the name of the discovered SIP trunk.
UCM Cluster	Indicates the name of the UCM cluster with which the SIP trunk is associated.
Device Pool	Indicates the name of the device pool with which the SIP trunk is associated. **Note:** To see the association with the device pool, you must configure the AXL credentials for the cluster to which the device pool is associated. For more information, see Configuring the NNM iSPI for IP Telephony to Access the AXL Data.

SIP Trunk Details Form

You can view the details of the selected SIP Trunk using the SIP Trunk Details form.

To view the SIP Trunk Details form, follow this step:

- From the SIP Trunk view table, select the SIP Trunk for which you want to view the details, and then click . The SIP Trunk Details form opens.

Analysis Pane

You can view a summary of the details of the selected SIP Trunk on the Analysis pane. The following tabs and related details are displayed:

SIP Trunk Details Summary tab

- SIP Trunk Name: The name of the SIP trunk.
- Cluster: The name of the UCM cluster.
- Device Pool Name: The name of the device pool.
- SIP trunk Remote CM List: The list of the remote CUCM servers.

SIP Trunk Session tab

Displays the details of the measurement types configured for the SIP Trunk Sessions. For more information about the measurement types configured for SIP Trunk Sessions, see Enabling the Monitoring of SIP Trunk Sessions.

SIP Trunk Details Form

The SIP Trunk Details form is split into two panes. The left pane displays the general attributes of the SIP Trunk. The right pane displays the following tabs:

- UCMs - displays the list of UCMs associated with the SIP Trunk. For more information about the **UCMs**tab, see Monitoring UCMs.
- Destinations - displays the IP address and the port details of the Cisco SIP trunk destination.
- Incidents - lists the incidents generated based on the state of the SIP trunk.

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
Name	The name of the SIP trunk.
Type	The type of Cisco SIP trunk.
UCM Cluster	The name of the UCM cluster to which the SIP trunk belongs.
Device Pool	The name of the device pool with which the SIP trunk is associated. To view the device pool details, click (the **Lookup** icon), and then click (the **Open** icon). The Device Pool Details form opens.

Analysis Pane

The Analysis pane displays a summary of the details of the selected SIP trunk. For more information, see Monitoring SIP Trunks.

Monitoring NTP Servers

The NTP Servers view displays the status of the Network Time Protocol (NTP) servers associated with a UCM cluster. The view arranges the key attributes of all associated NTP servers in a table.

To launch the Cisco NTP Servers view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest, and then click (the **Open** icon). The UCM Cluster Details form opens.
3. Click the NTP Servers tab. The NTP Servers view opens on the right pane.

Basic Attributes of the NTP Servers Table

Attribute	Description
Remote Server	Indicates the remote NTP server associated with the UCM cluster.
Stratum	Indicates the stratum number from the CUCM to the NTP remote server.
Reach	Indicates the peer reachability by the NTP process. This is reported as an octal value.
Offset	Indicates the frequency offset between the local clock hardware and the authoritative time from the NTP servers.
State	Indicates the state of the NTP server associated with the UCM cluster. The state can be one of the following: • Active: Indicates that the server is selected for synchronization • Rejected: Indicates that the server is discarded due to high stratum and failed sanity checks. • Selected: Indicates that the server is selected for sync, but has high delay/offset/jitter. • Included: Indicates that the server is a candidate NTP server and is included in the final selection set. • Invalid: Indicates that the server is invalid or non-viable.

NTP Server Details Form

You can view the details of the selected NTP Server using the NTP Server Details form.

To view the NTP Server Details form, follow this step:

- From the NTP Servers view table, select the NTP Server for which you want to view the details, and then click . The NTP Server Details form opens.

Analysis Pane

You can view a summary of the details of the selected NTP Server on the Analysis pane. The following tabs and related details are displayed:

NTP Server Details Summary tab

- Remote Server: The remote NTP server associated with the UCM cluster.
- Stratum: The stratum number from the CUCM to the NTP remote server.
- Reach: The peer reachability by the NTP process.
- Clock Offset: The frequency offset between the local clock hardware and the authoritative time from the NTP servers.
- Cluster NTP Status: The state of the NTP server associated with the UCM cluster.
- Management Server: The management server of the UCM subscriber group. This attribute displays one of the following values:
  - Local: If the UCM subscriber group is being managed by the NNMi management server console on which you are viewing the UCM subscriber group details.
  - Name of the regional manager that manages the UCM subscriber group.

Remote Server tab

This tab displays the following details of the selected NTP server associated with the UCM cluster:

- Remote Server
- Reach
- Clock Offset
- Cluster NTP Status

NTP Server Details Form

The NTP Server Details form is split into two panes. The left pane displays the general attributes of the NTP Server. The right pane displays the following tab:

- Incidents

General

The attributes that appear under the **General** section are described in the following table:

Attribute	Description
Remote Server	Indicates the remote NTP server associated with the UCM cluster.
Stratum	Indicates the stratum number from the CUCM to the NTP remote server.
Reach	Indicates the peer reachability by the NTP process. This is reported as an octal value.
Offset	Indicates the frequency offset between the local clock hardware and the authoritative time from the NTP servers.

Analysis Pane

The Analysis pane displays a summary of the details of the selected NTP Status. For more information, see Monitoring NTP Servers.

Monitoring Media Devices

The Media Devices view displays the media devices associated with a UCM cluster. You can monitor the following types of media devices:

- Cisco Annunciator Device
- Cisco Hardware (HW) Conference Bridge Device
- Cisco Music On Hold (MOH) Device
- Cisco Media Termination Point (MTP) Device
- Cisco Software (SW) Conference Bridge Device
- Cisco Transcode Device

To launch the Media Devices view, follow these steps:

1. From the **Workspaces** pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click Open. The UCM Cluster Details form opens.
3. Click the **Media Devices** tab. The Media Resources view opens on the right pane. You can see the monitored media devices in the cluster.

Basic Attributes of the Media Devices Table

Attribute	Description
Media Device Name	Indicates the name of the media device.
UCM Cluster	Indicates the name of Unified Communications Manager (UCM) cluster to which the selected media device is associated.
Device Pool	The name of the device pool to which the media device is associated. **Note:** To see the association with the device pool, you must configure AXL credentials for the cluster to which the device pool is associated. See the section Configuring Data Access for Cisco for more details.

Filtering Media Devices

You can filter the listed media devices in the Media Devices view based on the following attributes:

- Media Device Name
- UCM Cluster
- Device Pool

To filter the Media Devices view:

1. Right-click any of the listed attribute columns of one of the media devices listed in the Media Devices view and select **Filter**.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the media devices that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the media devices for which the selected column is not empty.
   - **Is empty**: filters and lists all the media devices for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the media devices that do not have the value in the column that you selected.The filtered list of media devices appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

You can view the details of a single media device in a form.

To view the Media Device Detail form:

Select a media device from the list of media resources displayed and click Open to open the Media Device Details Form. This form displays the attributes for the selected media device.

Analysis Pane

The Analysis pane provides a summary of the details of a selected media device as follows:

Media Device Details Summary tab

- Device Pool Name: The name of the device pool to which the selected media device is associated.
- UCM Cluster: The name of the UCM cluster to which the selected media device is associated.
- Management Server: The management server for the media device. This attribute displays one of the following values:
  - Local: If the media device is being managed by the NNMi management server console on which you are viewing the media device details.
  - Name of the regional manager that manages the media device.

General Information tab

- Description: A short description of the selected media device.
- Type: The type of the media device.
- IP Address: The IP address of the selected media device.

Media Resources Availability tab

- Total Resources: The number of resources present on the media device. The sum of available resources and active resources represents total resources.
- Available Resources: The number of resources that are available to be used. These resources are not in use at the current time.
- Active Resources: The number of resources that are currently in use.
- Unavailable Resources: The total number of unsuccessful attempts made to allocate a media resource from the device. The unsuccessful attempts occur when all media resources in the device are in use.

Media Device Details Form

The Media Device Details form helps you to view the details of the selected media device.

To launch the Media Device Details view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click Open. The UCM Cluster Details form opens.
3. Click the **Media Devices** tab, select a media device of your interest, and then click Open. The Media Device Details form opens.

The form displays the general attributes of the selected media device.

General Attributes

Attribute	Description
Type	The type of the media device..
Description	A short description of the media device.
IP Address	Indicates the IP address of the media device.
Device Pool Name	Indicates the name of the device pool to which the media device is associated.
Cluster Name	Indicates the name of Unified Communications Manager (UCM) cluster to which the selected media device is associated.

Analysis Pane

The Analysis pane displays a summary of the details of the selected media device. For more information, see Monitoring Media Devices.

Monitoring Voice Mail Devices

The Voice Mail Devices view displays the voice mail devices associated with a UCM cluster. The view arranges the details of all associated voice mail devices in a table.

To launch the Voice Mail Devices view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click Open. The UCM Cluster Details form opens.
3. Click the Voice Mail Devices tab. The Voice Mail Devices view opens on the right pane.

Voice Mail Device Details

Attribute	Description
Registration State	The registration state of the voice mail device with the UCM. The registration state can be Registered, Unregistered, Partially registered, Rejected or Unknown.
Name	The name of the voice mail device.
IP Address	The IP address of the voice mail device.
Description	The description of the voice mail device.

Analysis Pane

The Analysis pane of the voice mail device displays a summary of the details of the selected voice mail device as follows:

Cisco VM Port Details Summary tab

- Name: The name of the selected voice mail device.
- Cluster: The name of the UCM cluster with which the selected voice mail device is associated.
- Call Server: The UCM with which the selected voice mail device is registered.
- Device Pool: The name of the device pool with which the selected voice mail device is associated.
- Management Server: The management server for the voice mail device. This attribute displays one of the following values:
  - Local: If the voice mail device is being managed by the NNMi management server console on which you are viewing the voice mail device details.
  - Name of the regional manager that manages the voice mail device.

General Information tab

- IP Address: The IP address of the selected voice mail device.
- Registration State: The registration status of the selected voice mail device with its current UCM.

Monitoring Locations

The Locations view displays the details of the locations associated with a UCM cluster. The view arranges the key attributes of the Locations in a table.

To launch the Locations view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.

2. Select the UCM Cluster for which you want to launch the Locations view, and then click . The UCM Cluster Details form opens.

3. On the right pane of the form, click the **Locations** tab. The Locations view opens.

Basic Attributes of the Locations Table

Attribute	Description
Location Name	Indicates the name of the Location.
Audio Bandwidth (kbps)	Indicates the audio bandwidth value.

Location Details Form

You can view the details of the selected Location using the Location Details form.

To view the Location Details form, follow this step:

- From the Location view table, select the Location for which you want to view the details, and then click . The Location Details form opens.

Filtering Locations

You can filter the Locations, listed in the Locations view, using the available filters. This feature enables you to view the Locations based on the filter option that you selected. You can perform the filtering action on all the columns available on the Locations view table.

Note: You can select multiple filters based on your requirements.

To filter the Locations view, follow these steps:

1. Select a Location, listed in the Locations view, and right-click one of the following column attributes:
   - **Location Name**
   - **Audio Bandwidth (kbps)**
2. From the **Filter** option, select one of the following:
   - **Equals this value**: filters and lists all the Locations that have a value that is equal to the value of the column that you selected.
   - **Create filter...**: opens the **Filter** dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the Locations for which the selected column is not empty.
   - **Is empty**: filters and lists all the Locations for which the selected column is empty.

- **Not equal to this value**: filters and lists all the Locations that do not have the value in the column that you selected.

The filtered list of the Locations appears in the view.

After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Analysis Pane

You can view a summary of the details of the selected Location on the Analysis pane. The following tabs and related details are displayed:

- **Location Details Summary Tab**
  - Location Name: The name of the Location.
  - Cluster: The name of the UCM cluster to which the Location belongs.
  - Management Server: The management server for the selected Location. This attribute displays one of the following values:
    - **Local**: If the Location is being managed by the NNMi management server console on which you are viewing the Location details.
    - Name of the regional manager that manages the Location.
- **General Information Tab**
  - Location Name: The name of the Location.
  - Audio Bandwidth (kbps): The audio bandwidth value.
- **Locations Tab**
  - Out of Resources: The difference between the current and previous **Out of Resources** aggregate values for the configured polling interval. For example, if the aggregate value of the **Out of Resources** for a previous interval, for all the managed CMs in a cluster for a particular Cisco Location, is 10, and the current value is 12, the analysis pane displays the **Out of Resources** value as 2.

Location Details Form

The Location Details form helps you to view the general attributes of the selected Location.

General Attributes

Attribute	Description
Location Name	The name of the Location.
Audio Bandwidth (kbps)	The audio bandwidth value.

Analysis Pane

The Analysis pane displays a summary of the details of the selected Location. For more information, see Monitoring Locations.

Monitoring UCMEs

The UCMEs view displays a list of available Unified Call Manager Expresses (UCMEs) on the network. The view arranges the key attributes of all the discovered UCMEs in a table.

To launch the UCMEs view, follow this step:

- From the **Workspaces** navigation pane, click **Cisco IP Telephony** >**UCMEs**. The UCMEs view opens in the right pane.

Basic Attributes of the UCMEs Table

Attribute	Description
Name	The hostname of the UCME.
IP Address	The IP address of the UCME.
Tenant	The name of the tenant to which the UCME belongs.
Version	The version of the UCME.
Management Server	The management server for the UCME. This attribute displays one of the following values: • **Local**: If the UCME is being managed by the NNMi management server console on which you are viewing the UCME details. • Name of the regional manager that manages the UCME.

You can view the details of a single UCME in a form.

To view the Cisco Call Controller form, follow this step:

- From the Cisco Call Controllers view, select the node of your interest, and then click (Open). The Cisco Call Controller Details form opens.

To view the Node Form for the UCME, click , and then click **Open**. The Node Form opens displaying the details of the UCME.

Analysis Pane

The Analysis pane provides a summary of the details of a selected UCME as follows:

Cisco Call Controller Details Summary tab

- Name: The name of the selected UCME.
- Tenant: The name of the tenant to which the UCME belongs.

- Management Server: The management server for the UCME. This attribute displays one of the following values:
  - Local: If the UCME is being managed by the NNMi management server console on which you are viewing the UCME details.
  - Name of the regional manager that manages the UCME.

General Information tab

- Management Mode: The management status of the selected UCME.
- IP Address: The IP address of the selected UCME.
- Controller Type: The type of the selected UCME. For UCMEs, the only possible value for this field is Cisco Call Manager Express.
- Version: The version of the selected UCME.
- Description: A short description of the selected UCME.

Device Registrations tab

- Registered IP Phone Extensions: The number of IP phones associated with the selected UCME.
- Configured IP Phone Extensions: The number of IP phones managed by the selected UCME.

UCM Call Activity tab

This tab provides the count of the types of call activity on the UCME:

- Calls in Progress
- Completed Calls
- Incomplete Calls
- Attempted Calls
- Attempted System Calls
- Active Calls

Filtering UCMEs

You can filter the listed UCMEs in the UCMEs view based on the tenant and management server.

To filter the UCMEs view:, follow these steps

1. Right-click the **Management Server** or **Tenant** attribute column of one of the UCMEs listed in the UCMEs view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the UCMEs that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the UCMEs for which the selected column is not empty.
   - **Is empty**: filters and lists all the UCMEs for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the UCMEs that do not have the value in the column that you selected.

   The filtered list of UCMEs appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Cisco Call Controller Details Form

If you select a Unified Communication Manager (UCM), Survivable Remote Site Telephony (SRST) router, or Unified Call Manager Express (UCME) and click the Open icon, you can see the details of the selected UCM, UCME, or SRST router in the Cisco Call Controller Details form.

The Cisco Call Controller Details form helps you view the node details of the selected Cisco Call Controller server, the associated gatekeepers, the IP phones associated with it, and the IP phones configured with an SRST router. The form presents two different panes.

The right pane lists the following details:

- Gatekeepers: The Gatekeepers tab displays the details of all the gatekeepers associated with the selected Cisco Call Controller server. The tab displays the details of every associated gatekeeper in the format presented in the Cisco Gatekeepers view.
- Controlled IP Phones: The Controlled IP Phones tab displays the details of all the IP phones associated with the selected Cisco Call Controller server. The tab displays the details of every associated IP phone in the format presented in the Cisco IP Phones view.
- *Only visible when launched from the SRST Routers tab.* Configured IP Phones: The Configured IP Phones tab displays the list of IP phones configured with an SRST router. The tab displays the details of the IP phones registered with the SRST Router as shown in the SRST Router Configured IP Phones page.

- Incidents: The incidents generated for the Cisco Unified Communications Manager state changes.

The left pane lists the following details of the selected Cisco Unified Communications Manager.

Basic Attributes

Attribute	Description
Hosted Node	The node on which the Call Controller is hosted.
Name	The name of the Cisco Unified Communications Manager or SRST router.
IP Address	The IP address of the Call Controller server.
Management Mode	The management status of the node. The status can be any of the following strings: • Managed: indicates that the node is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the node is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the NNM iSPI for IP Telephony.
Type	The type of the Cisco Call Controller. The type can be one of the following: • Cisco Call Manager • Cisco Call Manager Express • SRST Router
Version	The version of the server.
Description	A short description of the server.

Call Manager Specific Attributes

Attribute	Description
UCM Cluster	Specifies the name of the Cisco Unified Communications Manager cluster.

Call Manager Specific Attributes, continued

Attribute	Description
CallManager Service State	The CallManager Service State of the selected Cisco Call Controller server. This attribute is not applicable for UCMEs. The possible values for a UCM are: • Up—indicates the selected UCM is UP • Down—indicates the selected UCM is DOWN • Unknown—indicates the SNMP response, which indicates the state of the UCM, is not available from the node. • Not Monitored—indicates the selected UCM is not currently monitored.

Only visible when launched from the SRST Router view. SRST Router Specific Attributes

Attribute	Description
E Phone Communication IP	The IP address of the SRST router interface that the E Phones use to communicate during a fallback.
SCCP Communication Port	The SCCP port that the phones use to communicate.
Max Conferences	The maximum number of conferences that can run simultaneously.
Max Directory Numbers	The maximum number of directory numbers that can be configured on the device.
Max E Phones	The maximum number of Ethernet phones (E phones) that can be registered with the device.
Voice Mail Number	The voicemail number configured for the device.
Total SCCP IP Phones Registered	The total number of SCCP IP Phones registered with the device.
Total SIP Phones Registered	The total number of SIP phones registered with the device.

Only visible when launched from the SRST Router view. SRST Router Specific Attributes, continued

Attribute	Description
State	The state of an SRST Router can be one of the following: • Active—indicates that the SRST router is in the active state and is the current call controller for the IP phones registered with the SRST Router. The SRST router state changes to active when the primary Call Controller for the registered phones is not available. • Standby—indicates that the SRST router is in the standby state and is not the current Call Controller for the IP Phones registered with the SRST Router. • Unknown—indicates the SNMP response, which indicates the state of the SRST router, is not available from the node. • Not Monitored—indicates the selected SRST router is not currently monitored.

Only visible when launched from the UCMEs view. **Call Manager Express Attributes**

Attribute	Description
EPhone Communication IP	The communication IP address used by the EPhone to communicate with the Call Manager Express.
SCCP Communication Port	The SCCP communication port used by EPhones to communicate with the Call Manager Express.
Max Conferences	The maximum number of conferences that can run simultaneously on the device.
Max Directory Numbers	The maximum number of directory numbers that you can configure with the device.
Max E Phones	The maximum number of E Phones that you can configure with the device.
Voice Mail Number	The voicemail number configured for the device.
Total SCCP IP Phones Registered	The total number of SCCP IP Phones registered with the Call Manager.

Analysis Pane

The Analysis pane provides a summary of the details of a selected Cisco Call Controller as follows:

Cisco Call Controller Details Summary tab

- Name: The name of the selected Cisco Call Controller.
- Management Address *(Only when launched from the UCMs view)*: The external (public) IP address of the selected UCM.
- Cluster *(Only when launched from the UCMs or SRST Routers view)*: The name of the cluster to which the UCM or SRST router belongs.
- Device Pool (Only when launched from the SRST Routers view): The name of the device pool with which the SRST router is associated.
- Tenant (Only when launched from the UCMEs view): The name of the tenant to which the UCME belongs.
- Management Server: The management server for the Cisco Call Controller. This attribute displays one of the following values:
  - Local: If the Cisco Call Controller is being managed by the NNMi management server console on which you are viewing the Cisco Call Controller details.
  - Name of the regional manager that manages Cisco Call Controller.

General Information tab

- Management Mode: The management status of the selected Cisco Call Controller.
- IP Address: The IP address of the selected Cisco Call Controller.
- Controller Type: The type of the selected Cisco Call Controller.
- Version: The version of the selected Cisco Call Controller.
- Description: A short description of the selected Cisco Call Controller.

Only when launched from the UCMEs or SRST Routers view. **Device Registrations tab**

- Registered IP Phones: The number of IP phones associated with the selected SRST router or Cisco Unified Communications Manager Express.
- Configured IP Phones: The number of IP phones configured with the SRST router.

Monitoring IP Phones

The IP Phones view displays a list of available Cisco IP phones on the network. The view arranges the key attributes of all discovered Cisco IP phones in a table.

To launch the IP Phones view:

From the **Workspaces** navigation pane, click **Cisco IP Telephony > IP Phones**. The IP Phones view opens on the right pane.

You can see the IP phones associated with a cluster from Cluster Details form.

To launch the IP Phones view from Cluster Details form, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a UCM Cluster of your interest and click (Open). The UCM Cluster Details form opens.
3. Click the IP Phones tab. The IP Phones view opens on the right pane.

Basic Attributes of the IP Phones Table

Attribute	Description
Registration State	The registration status of the Cisco IP phone line with its current controller. Possible values are as follows: • Registered • Unregistered • Unknown • Rejected
Extension Number	The extension number of the IP phone.
Model	The model of the IP phone.
Protocol	The protocol supported by the IP phone. The protocol can be Skinny Client Control Protocol (SCCP) or Session Initiation Protocol (SIP).
IP Address	The IP address of the IP phone.
Call Server	The call controller with which the IP phone is registered.
UCM Cluster	The name of the UCM cluster to which the IP phone is associated.
Tenant	The name of the tenant to which the IP phone belongs.
Device Pool	The name of the device pool to which the IP phone is associated.
SRST Router	The name of the Survivable Remote Site Telephony (SRST) router configured for the IP phone.

Basic Attributes of the IP Phones Table, continued

Attribute	Description
Management Server	The management server for the IP phone. This attribute displays one of the following values: • **Local**: If the IP phone is being managed by the NNMi management server console on which you are viewing the IP phone details. • Name of the regional manager that manages the IP phone.
Route Partition	The logical grouping of extension numbers and route patterns to which the shared line extension number belongs.
Shared Line	The extension number that is assigned to two or more IP phones. The extension number is part of the same route partition in all the IP phones.

When the status of a phone changes to *Unregistered*, the NNM iSPI for IP Telephony sends an incident to the NNMi incident browser.

You can view the details of a single IP phone in a form.

To view the Cisco Extension Details form:

From the IP Phones view, select the node of your interest, and then click (Open). The Cisco Extension Details form opens.

To view the Node Form for the IP phone, click , and then click **Open**. The Node Form opens displaying the details of the IP phone.

Viewing Cisco IP Telephony Reports

You can select an IP phone from the inventory and click **Actions** > **IP Telephony Reports** and select one of the following options to launch a chart detail report for the selected attribute:

- Average Duration of Calls Made
- Average Duration of Calls Received
- Termination Reasons for Calls Made
- Termination Reasons for Calls Received.

See the *NNM iSPI for IP Telephony Cisco IPT CDR Collection extension pack report online help* for more information.

Analysis Pane

The Analysis pane of the IP Phone displays a summary of the details of the selected IP Phone as follows:

Cisco Extension details Summary tab

- Name: The name of the selected IP phone.
- Cluster: The name of the UCM cluster to which the selected IP phone is associated.
- Call Server: The UCM with which the selected IP phone is registered.
- Tenant: The name of the tenant to which the IP phone belongs.
- Management Server: The management server for the IP phone. This attribute displays one of the following values:
  - Local: If the IP phone is being managed by the NNMi management server console on which you are viewing the IP phone details.
  - Name of the regional manager that manages the IP phone.

Extension Information tab

- Management Mode: The management status of the selected IP phone.
- Registration State: The registration status of the selected IP phone with its current UCM.
- IP Address: The IP address of the selected IP phone.
- MAC Address: The MAC address of the selected IP phone.
- Route Partition: The logical grouping of extension numbers and route patterns to which the shared line extension number belongs.
- Shared Line: The extension number that is assigned to two or more IP phones. The extension number is part of the same route partition in all the IP phones.
- Description: A short description of the selected IP phone.
- Model: The model of the selected IP phone.
- Device Pool: The name of the device pool to which the IP phone is associated.

Filtering Cisco IP phones

You can filter the listed IP phones in the IP Phones view with the available filters. You can perform the filtering action only on the **Registration State**, **IP Address**, **Extension Number**, **Route Partition**, **Shared Line**, **Tenant**, **Call Server**, **UCM Cluster**, **Device Pool**, **SRST Router**, or **Management Server** columns.

Note: You can select multiple filters based on your requirements.

To filter the IP Phones view, follow these steps:

1. Right-click the **Registration State**, **IP Address**, **Extension Number**, **Route Partition**, **Shared Line**, **Tenant**, **Call Server**, **SRST Router**, or **Management Server** attribute of one of the IP phones listed in the IP Phones view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the IP phones that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the IP Phones for which the selected column is not empty.
   - **Is empty**: filters and lists all the IP Phones for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the IP phones that do not have the value in the column that you selected.

The filtered list of Cisco IP phones appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Cisco Extension Details form

The Cisco Extension Details form helps you view the node details of the selected Cisco IP phone and the Cisco Call Controller servers associated with it. The form presents two different panes.

The right pane lists the following details:

- Current Controller: This tab displays the details of the Cisco Call Controller server that currently controls the selected Cisco IP Phone. The tab displays the details of the Cisco Call Controller in the format presented in the Call Controllers view .
- Previous Controller: The Previous Call Controllers tab displays the details of the Cisco Call Controller server that was previously controlling the selected Cisco IP phone. The tab displays the details of the Cisco Call Controller in the format presented in the Call Controllers view.
- Incidents: This tab displays the incidents generated for the IP phones.

The left pane lists the following details of the selected Cisco IP phone:

Basic Attributes of the Selected Cisco IP Phone

Attribute	Description
Hosted Node	The node on which the IP Phone is hosted.

Basic Attributes of the Selected Cisco IP Phone, continued

Attribute	Description
Extension Number	The extension number configured for the IP Phone.
Route Partition	The logical grouping of extension numbers and route patterns to which the shared line extension number belongs.
Shared Line	The extension number that is assigned to two or more IP phones. The extension number is part of the same route partition in all the IP phones.
Registration State	The registration status of the Cisco IP phone line with its current controller. Possible values are as follows: • Registered • Unregistered • Unknown • Rejected
IP Address	The IP address of the IP phone.
MAC Address	The MAC address of the Cisco IP phone.
Description	A short description of the phone.
Model	The model of the phone.
Management Mode	The management status of the node. The status can be any of the following strings: • Managed: indicates that the node is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the node is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the NNM iSPI for IP Telephony.
Protocol	The protocol used by the phone.
Device Pool	The name of the device pool to which the IP phone is associated.
SRST Router	The name of the SRST router.
Tenant	The name of the tenant to which the IP phone belongs.
Location	The location configured for the IP phone.

Basic Attributes of the Selected Cisco IP Phone, continued

Attribute	Description
Site Code	The site code configured for the IP phone.
Mail Code	The mail code configured for the IP phone.

Analysis Pane

The Analysis pane displays a summary of the details of the selected IP phone. For more information, see Monitoring IP Phones.

Updating Site Codes, Mail Codes, and Location Details of Cisco IP Phones

You can update the site code, mail code, and location of an IP phone from IP phone details form as follows:

1. Open the IP phone's details form.
2. Type the new site code, mail code, and location.
3. Save your changes.

Alternatively, you can update the site codes, mail codes, and locations of all Cisco IP phones on your network by using `nmsiptconfigimport.ovpl` command. You can import the new site codes, mail codes, and locations from a comma-separated values (CSV) file and update the IP phones with the new values.

To update the site codes, mail codes, and locations of Cisco IP phones from the command line, follow these steps:

1. Create a CSV file in the following format:

   ```
   Tenant,Cluster,Device Pool,IP Phone,Site code,Mail code,Location
   ```

   Note: The CSV file must have the following fields *in the same order* as mentioned here.

   a. **Tenant**: The name of the tenant to which the IP phone belongs. This is a not a mandatory field. If this field is kept empty, NNM iSPI for IP Telephony selects the default tenant.

   b. **Cluster**: The name of the cluster to which the IP phone is associated.

   c. **Device Pool**: The name of the device pool to which the IP phone is associated. This is not a mandatory field.

   d. **IP Phone**: You can use one of the following options to specify the details of IP phones:

- Using the actual extension numbers of IP phones. For example, if you want to update the site code, mail code, and location of the IP phone for the extension number 69750, specify 69750 in this field.
- Using the hyphen (-) to specify a range of IP phones. For example, if you want to update the IP phones with the extension numbers from 12300 to 52895, you can specify 12300-52895 in this field.
- Using the wildcard character percent (%) to specify a set of IP phones. The wildcard character percent (%) can match one or more digits. For example, if you want to update all the IP phones whose extensions numbers start with 8, you can specify as 8% in this field. If you want to update all the IP phones whose extensions numbers end with 8, you can specify %8 in this field. If you want to update all the IP phones whose extensions numbers start with 5 and end with 8, you can specify 5%8 in this field.
- Using the wildcard character question mark (?) to specify a set of IP phones. The wildcard character question mark (?) can match any single digit between 0 and 9. For example, if you want to update the IP phones with the extension numbers from 4830 to 4839, you can specify 483? in this field.

> **Note: IP Phone Range** is not a mandatory field. If this field is kept empty, the changes will be applied to all IP phones in the device pool or cluster.

e. **Site Code**: The new site code to be configured for the IP phones. You can use the keyword `UNSET` (case-sensitive) in this field to clear the current site codes and reset them to factory defaults, which are null.

f. **Mail Code**: The new mail code to be configured for the IP phones. You can use the keyword `UNSET` (case-sensitive) in this field to clear the current mail codes and reset them to factory defaults, which are null.

g. **Location**: The new location to be configured for the IP phones. You can use the keyword `UNSET` (case-sensitive) in this field to clear the current locations and reset them to factory defaults, which are null.

2. Log on to NNMi management server.
3. Run the following command:
   - On Windows

     ```
     %NnmInstallDir%\bin\nmsiptconfigimport.ovpl -type phonecustominfo -vendor cisco -u <user> -p <password> -f <csv_file>
     ```

   - On Linux

     ```
     /opt/OV/bin/nmsiptconfigimport.ovpl -type phonecustominfo -vendor cisco -u <user> -p <password> -f <csv_file>
     ```

In this instance, <user> is the NNMi user, <password> is the password of this user, and <*csv_file*> is the complete path name of the CSV file that contains the new site codes, mail codes, and locations of the IP phones.

See also Cisco Extension Details form.

Monitoring Cisco Gatekeepers

The Gatekeepers view displays a list of available Cisco gatekeeper devices on the network. The view arranges the key attributes of all gatekeepers in a table.

To launch the Cisco Gatekeepers view, follow this step:

- From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco Gatekeepers**. The Cisco Gatekeepers view opens in the right pane.

Basic Attributes of the Cisco Gatekeepers Table

Attribute	Description
Hosted Node	The hostname of the Cisco gatekeeper device.
IP Address	The IP address of the interface on the gatekeeper that communicates with other endpoints and gateways in the network.
Tenant	The name of the tenant to which the gatekeeper belongs.
H323Endpoints	The number of endpoints associated with the gatekeeper.
Management Server	The management server for the gatekeeper. This attribute displays one of the following values: ▪ **Local**: If the gatekeeper is being managed by the NNMi management server console on which you are viewing the gatekeeper details. ▪ Name of the regional manager that manages the gatekeeper.

You can view the details of a single Cisco gatekeeper in a form, which you can launch from the Cisco Gatekeepers view.

To view the Cisco Gatekeeper Details form, follow this step:

- From the Gatekeepers view, select the node of your interest, and then click . The Gatekeeper Details Form opens. The form displays details of the selected gatekeeper in the left pane, and details of all the associated Cisco CallManagers on the right pane.

To view the Node Form for the gatekeeper, click , and then click **Open**. The Node Form opens displaying the details of the gatekeeper.

Analysis Pane

The Analysis pane provides a summary of the details of a selected gatekeeper as follows:

Cisco Gatekeeper Details Summary tab

- IP Address: The IP address of the selected gatekeeper.
- Tenant: The name of the tenant to which the gatekeeper belongs.
- Management Server: The management server for the gatekeeper. This attribute displays one of the following values:
  - Local: If the gatekeeper is being managed by the NNMi management server console on which you are viewing the gatekeeper details.
  - Name of the regional manager that manages the gatekeeper.

GateKeeper Information tab

- Management Mode: The management status of the selected gatekeeper.
- Model: The model of the selected gatekeeper.
- H.323 Endpoints: The number of H.323 endpoints associated with the selected gatekeeper.
- Description: A short description of the selected gatekeeper.

Filtering Cisco Gatekeepers

You can filter the listed gatekeepers in the Gatekeepers view based on the management server.

To filter the Call Gatekeepers view, follow these steps:

1. Right-click the **Management Server** attribute column of one of the gatekeepers listed in the Gatekeepers view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the gatekeepers that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the gatekeepers for which the selected column is not empty.
   - **Is empty**: filters and lists all the gatekeepers for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the gatekeepers that do not have the value in the column that you selected.

     The filtered list of gatekeepers appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Cisco GateKeeper Details Form

The GateKeeper Details Form helps you view the node details of the selected Cisco GateKeeper device and the Cisco CallManager servers associated with it. The form presents two different panes.

The right pane lists the following information:

- UCMs: The UCMs tab displays the details of all the Cisco Unified Communications Managers associated with the selected gatekeeper device.

The left pane lists the following details of the selected Cisco gatekeeper device:

Basic Attributes of the Selected Cisco Gatekeeper Device

Attribute	Description
Hosted Node	The hostname of the gatekeeper.
IP Address	The IP address of the gatekeeper interface.
Description	A short description of the device.
Model	Model of the device.
H323 Endpoints	Number of H323 endpoints associated with the gatekeeper.
Management Mode	Displays the management state of the gatekeeper. The status can be one of the following strings: • Managed: indicates that the node is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the node is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the NNM iSPI for IP Telephony.

Monitoring Voice Gateways

The Voice Gateways view displays a list of available Cisco voice gateway devices in the network. The view arranges the key attributes of all discovered Cisco voice gateway devices in a table.

To launch the Cisco Voice Gateways view, follow this step:

- From the **Workspaces** navigation pane, click **Cisco IP Telephony > Voice Gateways**. The Cisco Voice Gateways view opens in the right pane.

Basic Attributes of the Cisco Voice Gateway Table

Attribute	Description
Operational State	The status of the Cisco voice gateway device. Possible values are: • No Status—the first polling cycle to collect the operational state has not taken place. • Normal—states of all associated circuit-switched interfaces with the voice gateway device are normal. • Unknown—states of all associated circuit-switched interfaces with the voice gateway device are unknown. • Warning—state of at least one associated circuit-switched interface is unknown; no associated circuit-switched interface is in the critical condition. • Minor—state of at least one (but not every) associated circuit-switched interface is critical. • Critical—state of every associated circuit-switched interface is critical. • Node Down—state of the voice gateway device is critical.
IP Address	The IP address of the Cisco voice gateway device.
Protocol	The protocol used by the gateway device.
UCM Cluster	The name of the UCM cluster to which the voice gateway belongs.
Device Pool	The name of the device pool to which the voice gateway is associated.
Call Server	The fully-qualified domain name of the Cisco CallManager device to which the voice gateway device is configured.
Custom Info	Indicates the custom information configured for the voice gateway.
Description	A description of the voice gateway device.
Management Server	The management server for the voice gateway device. This attribute displays one of the following values: • **Local**: If the voice gateway device is being managed by the NNMi management server console on which you are viewing the voice gateway device details. • Name of the regional manager that manages the voice gateway device.

Analysis Pane

The Analysis pane provides a summary of the details of a selected voice gateway as follows:

Voice Gateway Summary tab

- Name: The name of the selected voice gateway.
- Cluster: The name of the UCM cluster to which the selected voice gateway is associated.
- Device Pool: The name of the device pool to which the selected voice gateway is associated.
- Call Server: The fully-qualified domain name of the UCM device with which the selected voice gateway device is configured.

Voice Gateway Information tab:

- Management Mode: The management status of the selected voice gateway.
- IP Address: The IP address of the selected voice gateway.
- Operational State: The status of the selected voice gateway.
- Model: The model of the selected voice gateway.
- Protocol: The protocol configured for the selected voice gateway.
- Description: The description configured for the selected voice gateway.

Voice Gateway Interface Details tab:

- Number of Digital T1 CAS Interfaces: The number of digital T1 CAS interfaces in the selected voice gateway.
- Number of ISDN T1 PRI Interfaces: The number of ISDN T1 PRI interfaces in the selected voice gateway.
- Number of Digital E1 CAS Interfaces: The number of digital E1 CAS interfaces in the selected voice gateway.
- Number of ISDN E1 PRI Interfaces: The number of ISDN E1 PRI interfaces in the selected voice gateway.
- Number of Other Interfaces: The number of other interfaces in the selected voice gateway.

Filtering Cisco Voice Gateways

You can filter the listed Cisco Voice Gateways in the Voice Gateways view based on the following attributes:

- Operational State
- IP Address
- Protocol
- Call Server

Note: You can create filters for each of the listed attributes to view only the required voice gateways.

To filter the Voice Gateways view, follow these steps:

1. Right-click any of the listed attribute columns of one of the voice gateways listed in the Voice Gateways view and select **Filter**.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the voice gateways that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the voice gateways for which the selected column is not empty.
   - **Is empty**: filters and lists all the voice gateways for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the voice gateways that do not have the value in the column that you selected.

     The filtered list of voice gateways appears in the view.

   You can also filter the voice gateways by right clicking the attribute column headings and selecting **Filter** and one of the following options:

   - Is not empty
   - Is empty
   - Create Filter

All the attributes that you can use to filter are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to use to filter.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Filtering Voice Gateway Interfaces

You can filter the listed voice gateway interfaces in the Voice Gateway Interfaces tab page based on the following attributes of the voice gateway interfaces:

- Registration State
- Name
- Type
- CCM Device Name
- Usage State
- Custom Info
- Operational State

Note: You can create filters for each of the listed attributes to view only the required voice gateway interfaces.

To filter the voice gateway interfaces, follow these steps:

1. Right-click any of the listed attribute columns of one of the voice gateway interfaces listed in the Voice Gateway Interfaces tab page and select **Filter**.
2. Select one of the following filter options:
   - **Equals this value**: filters and lists all the voice gateway interfaces that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the voice gateway interfaces for which the selected column is not empty.
   - **Is empty**: filters and lists all the voice gateway interfaces for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the voice gateway interfaces that do not have the value in the column that you selected.

The filtered list of voice gateway interfaces appears in the view.

You can also filter the voice gateway interfaces by right clicking the attribute column headings and selecting **Filter** and one of the following options to filter the voice gateway interfaces:

- Is not empty
- Is empty
- Create Filter

Note:

- When you choose the **Create Filter** option, apart from the **Registration State**, the **Usage State**, and the **Operational State** columns, the other attribute columns are case sensitive. Make sure that you use the correct character case to specify the attribute values that you want to filter and view.
- After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Viewing Cisco Voice Gateway Endpoint Channels

You can launch a Node form from the Voice Gateway Interfaces tab to view the channel details of an endpoint of a Cisco Voice Gateway device. This node form includes an additional tab—the **Voice Gateway Channels** tab. The Voice Gateway Channels tab arranges all the key attributes of all the channels of the Cisco Gateway device endpoint in a table.

To launch the Node form to view endpoint channel details of a Cisco Voice Gateway device, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Voice Gateways**. The Voice Gateways view opens in the right pane.
2. In the right pane, click within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.
3. In this form, click the **Voice Gateway Interfaces** tab. You can view a list of discovered endpoints.
4. Click within the row representing the endpoint of your interest. The Node form opens. To view the channel details, click the **Voice Gateway Channels** tab.

Alternatively, follow these steps:

1. From the **Workspaces** navigation pane, click **Inventory > Nodes**. The Nodes view opens in the right pane. The Nodes view represents all the Cisco Voice Gateway devices (discovered by the NNM iSPI for IP Telephony) as nodes along with the other general nodes.

2. In the right pane, click within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.

3. In this form, click the **Voice Gateway Interfaces** tab. You can view a list of discovered endpoints.

4. Click within the row representing the endpoint of your interest. The Node form opens. To view the channel details, click the **Voice Gateway Channels** tab.

Analysis Pane

The Analysis pane provides a summary of the details of a selected gateway channel as follows:

Voice Gateway Channels Summary tab

- Name: The name of the selected channel.

Cisco VGW Channel Information tab

- Type: The type of the channel.
- Usage State: The usage state of the channel.

Monitoring Cisco Unity Devices

The Unity Devices view displays the details of the Cisco Unity devices in the network. The view arranges the key attributes of all discovered Cisco Unity devices in a table.

To launch the Cisco Unity Devices view, follow these steps:

From the **Workspaces** navigation pane, click **Cisco IP Telephony > Unity Devices**. The Cisco Unity Devices view opens in the right pane.

Basic Attributes of the Cisco Unity Devices Table

Attribute	Description
Name	Indicates the name of device.
Tenant	Indicates the name of the tenant to which the device belongs.
Version	Indicates the version of the device.
Management Server	The management server for the Cisco Unity Device. This attribute displays one of the following values: • **Local**: If the Cisco Unity device is being managed by the NNMi management server console on which you are viewing the call controller details. • Name of the regional manager that manages the Cisco Unity Device.

You can view the details of a single Cisco Unity device in a form.

To view the Cisco Unity device form, follow these steps:

In the Cisco Unity Devices view, select the node of your interest, and then click . The Cisco Unity Device Form opens.

To view the node form for the device, click and then click **Open**. The node form opens displaying the details of the device.

Analysis Pane

The Analysis pane provides a summary of the details of a selected unity device as follows:

Cisco Unity Details Summary tab

- Name: The name of the selected unity device.
- Tenant: The name of the tenant to which the unity device belongs.
- Management Server: The management server for the unity device. This attribute displays one of the following values:
  - Local: If the unity device is being managed by the NNMi management server console on which you are viewing the unity device details.
  - Name of the regional manager that manages the unity device.

General Information tab

- Management Mode: The management status of the selected device.
- IP Address: The IP address of the selected device.
- Version: The version of the selected device.

Filtering Cisco Unity Devices

You can filter the listed unity devices in the Unity Devices view based on the management server.

To filter the unity devices view:

1. Right-click the **Management Server** attribute column of one of the unity devices listed in the Unity Devices view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the unity devices that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.

- **Is not empty**: filters and lists all the unity devices for which the selected column is not empty.
- **Is empty**: filters and lists all the unity devices for which the selected column is empty.
- **Not equal to this value**: filters and lists all the unity devices that do not have the value in the column that you selected.

  The filtered list of unity devices appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Cisco Unity Devices Form

The Cisco Unity Devices Form displays the details of the selected Cisco Unity device.

Basic Attributes of the Cisco Unity Devices Table

Attribute	Description
Hosted Node	Indicates the node on which the Cisco Unity device is hosted.
Name	Indicates the name of device.
Version	Indicates the version of the device.
Management Mode	Indicates the management state of the device. The state can be one of the following: • Managed: indicates that the device is managed by the NNM iSPI for IP Telephony. • Out of Service: indicates that the device is currently out of service and not managed by the NNM iSPI for IP Telephony. • Unmanaged: indicates that the device is currently not managed by the NNM iSPI for IP Telephony.

Monitoring Configuration for Cisco Unified Communications Manager Clusters and Cisco Unified Communications Managers

The Monitoring Configuration feature enables you to monitor the state of additional attributes that indicate the health, performance, and availability of Cisco Unified Communications Managers, their

components, and associated devices. This feature also enables you to configure thresholds and generate incidents.

Note: This feature is not available for Cisco Unified Communications ManagerExpress systems (systems listed in the UCMEs inventory).

From each form that you open from the UCM Clusters inventory, you can open the Monitoring Configuration window by clicking **Actions > IP Telephony**. In the Monitoring Configuration window, you can select additional monitoring attributes for the selected device. You can view the states of these additional attributes in the following formats:

- Analysis pane in the inventory views
- Reports *(If you enable reporting)*
- *If you configure thresholds.* Incidents in the incidents inventory

Guidelines

- For the monitoring categories that are displayed at the cluster level, you must always configure the monitoring of measurement types for the Cisco Unified Communications Manager cluster, and then for the underlying Cisco Unified Communications Managers and components.
- Deleting a measurement type for a Cisco Unified Communications Manager cluster results in automatic deletion of the same measurement type for the underlying Cisco Unified Communications Managers.
- Threshold settings of a measurement type on a Cisco Unified Communications Manager cluster can be different from the threshold settings of the same measurement type on an underlying Cisco Unified Communications Manager.
- On a newly discovered Cisco Unified Communications Manager, UCM Subscriber Group, or device pool, you must manually enable the monitoring of the same measurement types that are configured for the other devices in the cluster.
- You cannot open multiple Monitoring Configuration windows at the same time. Before opening a new Monitoring Configuration window, make sure to click (the **Save** icon) in the existing Monitoring Configuration window to prevent loss of configuration data.

Note: In a Global Network Management (GNM) scenario, from the global manager console, you cannot add, delete, or disable the monitoring settings for the entities managed by the regional managers.

Monitoring UCM Call Activities

You can configure the NNM iSPI for IP Telephony to monitor call activities for a Cisco Unified Communications Manager. You can monitor the following activities:

Call Activity	Description
Calls in Progress	Indicates the number of voice or video calls currently in progress on the Cisco Unified Communications Manager. This includes the number of active calls as well.
Completed Calls	Indicates the number of calls that were connected and terminated through the Cisco Unified Communications Manager.
Incomplete Calls	Indicates the difference between the attempted calls and the completed calls.
Attempted Calls	Indicates the calls attempted. A call attempt occurs when the phone is taken from the hook and replaced back on the hook. A call attempt gets registered irrespective of the call being made. A call transfer or a conference attempt increments the number of attempted calls.
Attempted System Calls	Indicates the number of calls originating from the Cisco Unified Communications Manager and the attempted calls to the Unity Message Waiting Indicator.
Active Calls	Indicates the number of voice or video calls currently active and connected to the Cisco Unified Communications Manager.

Enabling the Monitoring of UCM Call Activity

The **Monitoring Configuration for UCM Cluster** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of Cisco Unified Communications Manager (CUCM) call activity. The page displays the list of existing UCM call activity configuration settings under the **UCM Call Activity** tab along with the attributes enabled and the thresholds set for each configured measurement. However, you can configure the UCM Call Activity settings only after configuring the SSH credentials for the Cisco Unified Communication Manager that you want to monitor. For more information about configuring SSH credentials, see Accessing the Cisco Unified Communications Manager with SSH.

To enable the monitoring of UCM Call Activity, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters** from the list of options. This displays the UCM Clusters view.
3. From the UCM Clusters view, select a cluster, and then click **Actions** > **IP Telephony** > **Monitoring Configuration**. The Monitoring Configuration for UCM Cluster page opens.

   Alternatively, right-click a cluster in the UCM Clusters view, and then click **IP Telephony > Monitoring Configuration**.
4. On the left pane of the **Monitoring Configuration for UCM Cluster** page, select **UCM Call Activity** from the **Area of Monitoring** drop-down list.

5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the UCM Call Activity Settings.

6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the Call Activity setting, go to **Step 5**.

7. On the left pane of the page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Collection Interval	Select minutes (**mins**) or hours (**hrs**) from the drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to monitor the UCM call activity for the cluster periodically.
Apply Configuration Setting to Other UCM Clusters	Select this option if you want the UCM call activity monitoring settings to be applied on other clusters.

8. Click (the **Save** icon) to save the monitoring configuration.

You can select a Cisco Unified Communications Manager from the **Call Controller Details** form and click **Actions** > **IP Telephony** > **Monitoring Configuration** from the menu to launch the Monitoring Configuration for UCM Call Activity page for the selected Cisco Unified Communications Manager. However, you cannot specify the data collection intervals if you launch the Monitoring Configuration form for a particular Cisco Unified Communications Manager—you must always specify the collection intervals at the cluster level. Individual Cisco Unified Communications Managers assume the intervals specified for the corresponding cluster.

To modify an existing UCM Call Activity configuration setting, follow these steps:

1. Select the UCM Call Activity configuration that you want to modify, and then click **Edit**. The **Add/Update UCM Call Activity** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing UCM Call Activity configuration setting, follow this step:

- Select the Call Activity configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing UCM Call Activity configuration settings.

To disable an existing UCM Call Activity configuration setting, follow this step:

- Select the UCM Call Activity configuration that you want to disable, and then click **Disable All**.

Note: The **Delete**, **Delete All**, and **Disable All** buttons are enabled only at the **UCM Cluster**

level.

Configuring the UCM Call Activity Settings

The **Add/Update UCM Call Activity** page enables you to define the attributes for configuring the UCM Call Activity settings specifying threshold settings to generate incidents, and enabling monitoring and reporting for UCM call activity.

To configure the UCM Call Activity settings, follow these steps:

1. On the **Add/Update UCM Call Activity** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the UCM Call Activity type that is to be monitored. You can select one of the following types of measurement: ▪ **Calls in Progress** ▪ **Completed Calls** ▪ **Incomplete Calls** ▪ **Attempted Calls** ▪ **Attempted System Calls** ▪ **Active Calls** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ■ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ■ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ■ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ■ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the UCM Call Activity type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the UCM Call Activity type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the UCM call activity configuration settings.

Monitoring Registered Devices Count

You can monitor the count of various registered devices based in a cluster. When you configure the monitoring of registered devices counts for a cluster, the configuration settings are automatically applied to all the UCM subscriber groups, Cisco Unified Communications Managers, and the device pools in the cluster. The NNM iSPI for IP Telephony enables you to monitor the count of the following registered devices:

- Analog Access Gateway Boxes
- CTI Ports
- CTI Route Points
- H.323 Gateway Boxes
- Hardware Phones
- Media Resources
- MGCP/SCCP EANDM
- MGCP/SCCP FXO
- MGCP/SCCP FXS
- MGCP/SCCP Gateway Endpoints
- MGCP/SCCP T1/E1 CAS
- MGCP/SCCP T1/E1 PRI
- Other IP Phones
- **Other Station Devices**[1]
- VM Ports

Note: You can get the exact counts of the newly configured hardware phones and other IP phones immediately after they are added to the network. The exact counts of all other devices, which are configured newly, will be available only after the next scheduled discovery of theNNM iSPI for IP Telephony.

[1]The counts of the Soft IP Phones, VM Ports, CTI Route Points, and CTI Ports are summed up to calculate the count of Other Station Devices.

Enabling the Monitoring of Registered Devices Count

The **Monitoring Configuration for UCM Cluster** page of the NNM iSPI for IP Telephony helps you to enable the monitoring the counts of Cisco Unified Communications Managerregistered devices. The page displays the list of existing registered device count configuration settings under the **Registered Devices Count** tab along with the measurement types enabled and the thresholds set for each configured measurement. However, you can configure the Registered Devices Count settings only after configuring the SSH credentials for the Cisco Unified Communication Manager that you want to monitor. For more information about configuring SSH credentials, see Configuring SSH Access for a Cisco Unified Communications Manager Cluster.

To enable the monitoring of Registered Device Count, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view.
3. From the UCM Clusters view, select a cluster, and then click **Actions** > **IP Telephony** > **Monitoring Configuration**. The Monitoring Configuration for UCM Cluster page opens.

   Alternatively, right-click a cluster in the UCM Clusters view, and then click **IP Telephony > Monitoring Configuration**.
4. On the left pane of the **Monitoring Configuration for UCM Cluster** page, select **Registered Devices Count** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click * (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the Registered Devices Count Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the Registered Devices Count setting, go to **Step 5**.
7. On the left pane of the page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Collection Interval	Select minutes (**mins**) or hours (**hrs**) from the drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to monitor the counts of the registered devices for the cluster periodically.
CSV Export Interval	Select minutes (**mins**) or hours (**hrs**) from the drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to export the counts of the monitored devices for the cluster periodically.

Apply Configuration Setting to Other UCM Clusters	Select this option if you want the registered device count monitoring settings to be applied on other clusters.

8. Click (the **Save** icon) to save the monitoring configuration.

You can also launch Monitoring Configuration form for a UCM subscriber group, UCM, or device pool from the details forms of a UCM subscriber group, UCM, or device pool. If you launch the Monitoring Configuration form for a UCM subscriber group, UCM, or device pool, you cannot add a new registered device count monitoring configuration or delete an existing registered device count monitoring configuration, and you cannot enable or disable monitoring. However, you can modify the threshold settings from these forms, and enable or disable CSV export.

To modify an existing Registered Device Count configuration setting, follow these steps:

1. Select the registered device count configuration that you want to modify, and then click **Edit**. The **Add/Update Registered Devices Count** page opens.
2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing Registered Device Count configuration setting, follow this step:

- Select the registered device count configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing registered device count configuration settings.

To disable an existing Registered Device Count configuration setting, follow this step:

- Select the registered device count configuration that you want to disable, and then click **Disable All**.

Note: The **Delete**, **Delete All**, and **Disable All** buttons are enabled only at the **UCM Cluster** level.

Configuring the Registered Devices Count Settings

The **Add/Update Registered Devices Count** page enables you to define the attributes for configuring the Registered Devices Count settings specifying threshold settings to generate incidents, enabling monitoring for the counts of Cisco Unified Communications Managerregistered devices, and enabling CSV export for the registered devices. When you configure the monitoring of registered device count for a cluster, the configuration settings are automatically applied to all Cisco Unified Communications Manager subscriber groups, Cisco Unified Communications Managers, and device pools in the cluster.

To configure the Registered Devices Count settings, follow these steps:

1. On the **Add/Update Registered Devices Count** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the Device type that is to be monitored. You can select one of the following types of measurement: ▪ **Analog Access Gateway Boxes** ▪ **CTI Ports** ▪ **CTI Route Points** ▪ **H.323 Gateway Boxes** ▪ **Hardware Phones** ▪ **Media Resources** ▪ **MGCP/SCCP EANDM** ▪ **MGCP/SCCP FXO** ▪ **MGCP/SCCP FXS** ▪ **MGCP/SCCP Gateway Endpoints** ▪ **MGCP/SCCP T1/E1 CAS** ▪ **MGCP/SCCP T1/E1 PRI** ▪ **Other IP Phones** ▪ **Other Station Devices**[1] ▪ **VM Ports** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.

[1]The counts of the Soft IP Phones, VM Ports, CTI Route Points, and CTI Ports are summed up to calculate the count of Other Station Devices.

Enable CSV Export	Select the check box to enable CSV export for the selected Measurement Type. The NNM iSPI for IP Telephony places the CSV files into the following directory on the NNMi management server: ■ On Windows: `%nnmdatadir%\shared\ipt\CSVExport\Cisco\RegisteredDevicesCount` ■ On UNIX/Linux: `/var/opt/OV/shared/ipt/CSVExport/Cisco/RegisteredDevicesCount` To use the CSV files, you must have sufficient privilege to access the above location.
Generate Incident	Select the check box to generate incident in the incident inventory.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ■ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ■ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ■ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ■ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the Device type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.

Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the Device type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the registered devices count configuration settings.

Monitoring Gateway Call Activity

You can configure the NNM iSPI for IP Telephony to monitor gateway call activities of a Cisco Unified Communications Manager and the following types of gateway entities:

- H.323 Gateway Box
- MGCP/SCCP Gateway Interfaces

You can configure the following measurement types for monitoring the Gateway Call Activity:

- Gateway Active Calls: Indicates the active calls handled by the gateways in your network.
- Gateway Current Active Calls: Indicates the channels that are currently active in the H.323 gateways and the MGCP gateway interfaces in your network.

Enabling the Monitoring of Gateway Call Activity

The **Monitoring Configuration for UCM Cluster** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of Cisco Unified Communications Managergateway call activity. The page displays the list of existing gateway call activity configuration settings under the **Gateway Call Activity** tab along with the attributes enabled and the thresholds set for each configured measurement. However, you can configure the Gateway Call Activity settings only after configuring the SSH credentials for the Cisco Unified Communication Manager that you want to monitor. For more information about configuring SSH credentials, see Configuring SSH Access for a Cisco Unified Communications Manager Cluster.

To enable the monitoring of Gateway Call Activity, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view.
3. From the UCM Clusters view, select a cluster, and then click **Actions** > **IP Telephony** > **Monitoring Configuration**. The Monitoring Configuration for UCM Cluster page opens.

   Alternatively, right-click a cluster in the UCM Clusters view, and then click **IP Telephony > Monitoring Configuration**.
4. On the left pane of the **Monitoring Configuration for UCM Cluster** page, select **Gateway Call Activity** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the Gateway Call Activity Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the gateway call activity settings, go to **Step 5**.
7. On the left pane of the page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Collection Interval	Select minutes (**mins**) or hours (**hrs**) from the drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to monitor the gateway call activity for the cluster periodically.
Apply Configuration Setting to Other UCM Clusters	Select this option if you want the gateway call activity monitoring settings to be applied on other clusters.

8. Click (the **Save**icon) to save the monitoring configuration.

An H.323 gateway that is associated to more than one cluster, assumes the data collection intervals specified for the corresponding cluster to which it is associated. You cannot specify the data collection intervals for a gateway by launching the Monitoring Configuration form from the Voice Gateway Details form.

To modify an existing Gateway Call Activity configuration setting, follow these steps:

1. Select the Gateway Call Activity configuration that you want to modify, and then click **Edit**. The **Add/Update Gateway Call Activity** page opens.
2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing Gateway Call Activity configuration setting, follow this step:

- Select the Gateway Call Activity configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing Gateway Call Activity configuration settings.

To disable an existing Gateway Call Activity configuration setting, follow this step:

- Select the Gateway Call Activity configuration that you want to disable, and then click **Disable All**.

Note: The **Delete**, **Delete All**, and **Disable All** buttons are enabled only at the cluster level.

You can select a gateway interface from the **Voice Interfaces Gateway** form to configure the monitoring of active calls on the selected gateway interface.

Note: You can configure the active call monitoring at the gateway interface level only if you have configured the same at the cluster level.

To configure the monitoring of Gateway Call Activity for a gateway interface, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select the cluster for which you want to launch the **Voice Interfaces Gateway** form, and then click . The UCM Cluster Details form opens.
3. On the right pane of the form, click the **H.323 Gateways** or the **MGCP/SCCP Gateways** tab based on your requirement to monitor the active calls. The respective view opens.
4. Select the gateway interface for which you want to enable the monitoring, and then click . The **Voice Interfaces Gateway** form opens.
5. Click **Actions** > **IP Telephony** > **Monitoring Configuration**. The **Monitoring Configuration for Cisco Voice Gateway Interface**, with the page opens.
6. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the Gateway Call Activity Settings.

   Note: At the gateway interface level, you can configure active call monitoring only for those interfaces that were configured for the same at the cluster level.

7. Click (the **Refresh** icon) to view the newly-added measurement type.
8. Click (the **Save**icon) to save the monitoring configuration.

Configuring the Gateway Call Activity Settings

The **Add/Update Gateway Call Activity** page enables you to define the attributes for configuring the Gateway Call Activity settings such as specifying threshold settings to generate incidents and enabling monitoring for gateway call activity. When you configure the monitoring of gateway call activity for a cluster, the configuration settings are automatically applied to all the H.323 and MGCP/SCCP gateway interfaces in the cluster.

To configure the Gateway Call Activity settings, follow these steps:

1. On the **Add/Update Gateway Call Activity** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the Gateway Call Activity type that is to be monitored. You can select one of the following types of measurement: ▪ **Gateway Active Calls** ▪ **Gateway Current Active Calls**
Enable Collection	Select the check box to enable collection of the selected measurement type.
Enable Reporting	Select the check box to enable reporting of the selected measurement type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ■ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ■ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ■ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ■ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the Gateway Call Activity type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the Gateway Call Activity type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the gateway call activity configuration settings.

Monitoring Route List and Hunt List Count Configurations

You can configure the NNM iSPI for IP Telephony to monitor the route list and hunt list counts for a Cisco Unified Communications Manager. A route list is a set of route groups arranged in a specific order responsible for regulating the available devices for outgoing calls. A hunt list is a set of line groups arranged in a specific order responsible for regulating the available directory numbers for incoming calls.

Enabling the Monitoring of Route List and Hunt List Count Configurations

The **Monitoring Configuration for UCM Cluster** page of the NNM iSPI for IP Telephony helps you to enable the monitoring the counts of Cisco Unified Communications Managerroute list and hunt list configurations. The page displays the list of existing route list and hunt list count configuration settings under the **Configurations** tab along with the attributes enabled and the thresholds set for each configured measurement. However, you can configure the route list and hunt list count settings only after configuring the AXL credentials for the cluster that you want to monitor. For more information about configuring AXL credentials, see Configuring AXL Data Access for a Cisco Unified Communications Manager Cluster.

Monitoring of the count of route lists and hunt lists enables you to configure thresholds for the monitored devices. The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreach* incidents when the thresholds are violated.

To enable the monitoring of route list or hunt list count, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view.
3. From the UCM Clusters view, select a cluster, and then click **Actions** > **IP Telephony** > **Monitoring Configuration**. The Monitoring Configuration for UCM Cluster page opens.

   Alternatively, right-click a cluster in the UCM Clusters view, and then click **IP Telephony > Monitoring Configuration**.
4. On the left pane of the **Monitoring Configuration for UCM Cluster** page, select **Configurations** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the Route List and Hunt List Count Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the route list and hunt list count setting, go to **Step 5**.
7. On the left pane of the page, specify the required details in the fields provided on the page. The

following table describes the fields on the page:

Field Name	Description
Collection Interval	Select minutes (**mins**) or hours (**hrs**) from the drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to monitor the counts of the route lists and hunt lists for the cluster periodically.
CSV Export Interval	Select minutes (**mins**) or hours (**hrs**) from the drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to export the counts of the route lists and hunt lists for the cluster periodically.
Apply Configuration Setting to Other UCM Clusters	Select this option if you want the route lists and hunt lists count monitoring settings to be applied on other clusters.

8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing route list or hunt list count configuration setting, follow these steps:

1. Select the route list or hunt list count configuration that you want to modify, and then click **Edit**. The **Add/Update Configurations** page opens.
2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing route list or hunt list count configuration setting, follow this step:

- Select the route list or hunt list count configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing registered device count configuration settings.

To disable an existing route list or hunt list count configuration setting, follow this step:

- Select the route list or hunt list count configuration that you want to disable, and then click **Disable All**.

Note: The **Delete**, **Delete All**, and **Disable All** buttons are enabled only at the **UCM Cluster** level.

Configuring the Route List and Hunt List Count Settings

The **Add/Update Configurations** page enables you to define the attributes for configuring the route list count or hunt list count settings specifying threshold settings to generate incidents,

enabling monitoring for the counts of Cisco Unified Communications Managerroute list and hunt list, and enabling CSV export for the route list and hunt list.

To configure the route list count or hunt list count settings, follow these steps:

1. On the **Add/Update Configurations** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the Configuration type that is to be monitored. You can select one of the following types of measurement: ▪ **Route List** ▪ **Hunt List** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable CSV Export** check boxes to enable collection and csv exporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable CSV Export	Select the check box to enable CSV export for the selected Measurement Type. The NNM iSPI for IP Telephony places the CSV files into the following directory on the NNMi management server: ▪ On Windows: `%nnmdatadir%\shared\ipt\CSVExport\Cisco\RegisteredDevicesCount` ▪ On UNIX/Linux: `/var/opt/OV/shared/ipt/CSVExport/Cisco/RegisteredDevicesCount` To use the CSV files, you must have sufficient privilege to access the above location.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the Configuration type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the Configuration type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the route list or hunt list count configuration settings.

Monitoring Media Resource Activity

You can configure the NNM iSPI for IP Telephony to monitor the media resources in each cluster. You can configure media resource activity monitoring for a cluster as well as for a media device.When you configure the monitoring for media resources of a cluster, the configuration settings are automatically applied to all the media devices in the cluster. You can monitor the following activities:

Media Resource Activity	Description
Active Resources	Indicates the number of resources that are currently in use.
Unavailable Resources	Indicates the number of unsuccessful attempts made to allocate a media resource from the device. The unsuccessful attempts occur when all media resources in the device are in use.
Available Resources	Indicates the number of resources that are available to be used. These resources are not in use at the current time.
Total Resources	Indicates the total number of media resources.

Enabling the Monitoring of Media Resource Activity

The **Monitoring Configuration for UCM Cluster** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the media resource activity in each cluster. The page displays the list of existing media resource activity configuration settings under the **Media Resource Activity** tab along with the attributes enabled and the thresholds set for each configured measurement. However, you can configure the Media Resource Activity settings only after configuring the SSH credentials for the Cisco Unified Communication Manager that you want to monitor. For more information about configuring SSH credentials, see Configuring SSH Access for a Cisco Unified Communications Manager Cluster.

To enable the monitoring of media resource activity, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view.
3. From the UCM Clusters view, select a cluster, and then click **Actions** > **IP Telephony** > **Monitoring Configuration**. The Monitoring Configuration for UCM Cluster page opens.

   Alternatively, right-click a cluster in the UCM Clusters view, and then click **IP Telephony > Monitoring Configuration**.

4. On the left pane of the **Monitoring Configuration for UCM Cluster** page, select **Media Resource Activity** from the **Area of Monitoring** drop-down list.

5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the Media Resource Activity Settings.

6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the Media Resource Activity setting, go to **Step 5**.

7. On the left pane of the page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Collection Interval	Select minutes (**mins**) or hours (**hrs**) from the drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to monitor the media resource activity for the cluster periodically.
Apply Configuration Setting to Other UCM Clusters	Select this option if you want the media resource activity monitoring settings to be applied on other clusters.

8. Click (the **Save** icon) to save the monitoring configuration.

You can select a media device from the **Media Device Details** form and click **Actions** > **IP Telephony** > **Monitoring Configuration** from the menu to launch the Monitoring Configuration for Cisco Media Device page for the selected media device. You can add a new Media Resource Activity monitoring configuration for a media device from the **Media Device Details** form only if you have added the same configuration at the cluster level. However, you can add monitoring configurations for the new media devices added to the topology after you configured the Media Resource Activity monitoring for the cluster.

To modify an existing Media Resource Activity configuration setting, follow these steps:

1. Select the Media Resource Activity configuration that you want to modify, and then click **Edit**. The **Add/Update Media Resource Activity** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing Media Resource Activity configuration setting, follow this step:

- Select the Media Resource Activity configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing Media Resource Activity configuration settings.

To disable an existing Media Resource Activity configuration setting, follow this step:

- Select the Media Resource Activity configuration that you want to disable, and then click **Disable All**.

Note: The **Delete**, **Delete All**, and **Disable All** buttons are enabled only at the **UCM Cluster** level.

Configuring the Media Resource Activity Settings

The **Add/Update Media Resource Activity** page enables you to define the attributes for configuring the media resource activity settings specifying threshold settings to generate incidents, enabling monitoring, and enabling reporting for the media devices.

To configure the media resource activity settings, follow these steps:

1. On the **Add/Update Media Resource Activity** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the Media Resource type that is to be monitored. You can select one of the following types of measurement: ▪ **Active Resources** ▪ **Unavailable Resources** ▪ **Available Resources** ▪ **Total Resources** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.

Generate Incident	Select the check box to generate incident in the incident inventory. **Note:** The **Generate Incident** check box is disabled at the cluster level. You can set thresholds to generate incidents for a device at the media device level. You can select a media device from the **Media Device Details** form and click **Actions** > **IP Telephony** > **Monitoring Configuration** from the menu to launch the Monitoring Configuration for Cisco Media Device page for the selected media device.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ■ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ■ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ■ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ■ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the Media Resource type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the Media Resource type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.

Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the media resource activity configuration settings.

Monitoring CTIManager Connections Count

You can configure the NNM iSPI for IP Telephony to monitor the active connections count of the AXL CTIManager for a Cisco Unified Communications Manager (CUCM). You can monitor the following activities:

CTIManager Connections Count	Description
CTIConnectionActive	Indicates the total number of CTI clients that are currently connected to the CTIManager. While the CTIConnectionActive count increases by one when a new connection is established, the count decreases by one when a connection is released.
Ccm LinkActive	Indicates the total number of active CUCM links. The CTIManager maintains links to all the active CUCM in the cluster.
Devices Open	Indicates the total number of devices such as hardware IP phones, CTI ports, and CTI route points that are configured in the CUCM that the CTI applications control and monitor.
Lines Open	Indicates the total number of lines that are configured in the CUCM that control and monitor the CTI applications.

Note: To enable the monitoring of these attributes, you must also turn on the CTIManager service on the CUCMs.

Enabling the Monitoring of CTIManager Connections Count

The **Monitoring Configuration for UCM Cluster** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the CTIManager Connections Count. The page displays the list of the existing configuration settings under the **CTIManager Connections Count** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of CTIManager Connections Count, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view.
3. From the UCM Clusters view, select a cluster, and then click **Actions** > **IP Telephony** > **Monitoring Configuration**. The Monitoring Configuration for UCM Cluster page opens.

   Alternatively, right-click a cluster in the UCM Clusters view, and then click **IP Telephony > Monitoring Configuration**.
4. On the left pane of the **Monitoring Configuration for UCM Cluster** page, select **CTIManager Connections Count** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the CTIManager Connections Count Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the CTIManager Connections Count setting, go to **Step 5**.
7. On the left pane of the page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Collection Interval	Select minutes (**mins**) or hours (**hrs**) from the drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to monitor the connections count for the CTIManager periodically.
Apply Configuration Setting to Other UCM Clusters	Select this option if you want the CTIManager connections count monitoring settings to be applied on other clusters.

8. Click (the **Save** icon) to save the monitoring configuration.

You can select a Cisco Unified Communications Manager from the **Call Controller Details** form and click **Actions** > **IP Telephony** > **Monitoring Configuration** from the menu to launch the Monitoring Configuration for the CTIManager Connections Count page for the selected Cisco Unified Communications Manager. However, you cannot specify the data collection intervals if you launch the Monitoring Configuration form for a particular Cisco Unified Communications Manager—you must always specify the collection intervals at the cluster level. Individual Cisco Unified Communications Managers assume the intervals specified for the corresponding cluster.

To modify an existing CTIManager Connections Count configuration setting, follow these steps:

1. Select the CTIManager Connections Count configuration that you want to modify, and then click **Edit**. The **Add/Update CTIManager Connections Count** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing CTIManager Connections Count configuration setting, follow this step:

- Select the CTIManager Connections Count configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing CTIManager Connections Count configuration settings.

To disable an existing CTIManager Connections Count configuration setting, follow this step:

- Select the CTIManager Connections Count configuration that you want to disable, and then click **Disable All**.

Note: The **Delete**, **Delete All**, and **Disable All** buttons are enabled only at the **UCM Cluster** level.

Configuring the CTIManager Connections Count Settings

The **Add/Update CTIManager Connections Count** page enables you to define the attributes for configuring the CTIManager Connections Count settings specifying threshold settings to generate incidents, and enabling monitoring and reporting for the active connections of the CTIManager.

To configure the CTIManager Connections Count settings, follow these steps:

1. On the **Add/Update CTIManager Connections Count** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the CTIManager Connections Count type that is to be monitored. You can select one of the following types of measurement: ▪ **CTIConnectionActive** ▪ **Ccm LinkActive** ▪ **Devices Open** ▪ **Lines Open** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.

Lower Base	Specify the lower base value for the CTIManager Connections Count type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the CTIManager Connections Count type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Monitoring Locations

You can configure the NNM iSPI for IP Telephony to monitor the Cisco Locations at the UCM Cluster and Locations levels. You can configure the following type of measurement attribute for monitoring Locations:

- Out Of Resources: Indicates the total number of times that a call on a particular Cisco Unified Communications Manager (CUCM) through the location failed due to lack of bandwidth.

Note: In a CUCM 9x cluster, the **Out Of Resources** measurement attribute is not available for the pre-configured Cisco Locations such as **Phantom** and **Shadow**.

Enabling the Monitoring of Locations

The **Monitoring Configuration for UCM Cluster** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of Locations. The page displays the list of existing Locations configuration settings under the **Locations** tab along with the attributes enabled and the thresholds set for each configured measurement. However, you can configure the Locations settings only after configuring the SSH credentials for the Cisco Unified Communication Manager that you want to

monitor. For more information about configuring SSH credentials, see Configuring SSH Access for a Cisco Unified Communications Manager Cluster.

To enable the monitoring of Locations, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters**. The UCM Clusters view opens.
3. Select a UCM Cluster of your interest and click **Actions** > **IP Telephony** > **Monitoring Configuration**. The **Monitoring Configuration for UCM Cluster** page opens.

   Tip: Alternatively, you can also launch the Monitoring Configuration page for locations from the Location Details form. If you launch the Monitoring Configuration page for locations, you cannot do the following:

   - Add a new location monitoring configuration
   - Delete an existing location monitoring configuration
   - Enable or disable monitoring

   However, you can add the threshold settings only at the Location Details form level.
4. On the left pane of the **Monitoring Configuration for UCM Cluster** page, select **Locations** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the Locations Settings.
6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the Locations setting, go to **Step 5**.
7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the Locations for the UCM Cluster. The default value is five minutes. You can select only a value that is greater than the default value.
8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing Locations configuration setting, follow these steps:

1. Select the Location configuration that you want to modify, and then click **Edit**. The **Add/Update Location** page opens.
2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing Locations configuration setting, follow this step:

- Select the Location configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing Location configuration settings.

To disable an existing Locations configuration setting, follow this step:

- Select the Location configuration that you want to disable, and then click **Disable All**.

Note: The **Delete**, **Delete All**, and **Disable All** buttons are enabled only at the **UCM Cluster** level.

Configuring the Locations Settings

The **Add/Update Location** page enables you to define the attributes for configuring Locations.

To configure Locations settings, follow these steps:

1. On the **Add/Update Location** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the Location type that is to be monitored. The following type is available: ▪ **Out Of Resources**
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
The following fields are enabled only at the Location Details form level:	
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the Locations type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the Locations type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Monitoring SIP Trunk Sessions

You can configure the NNM iSPI for IP Telephony to monitor the SIP trunk sessions for a Cisco Unified Communications Manager (CUCM). You can monitor the following activities:

SIP Trunk Sessions	Description
Active Calls	Indicates the total number of active calls on the SIP Trunk Session.
Attempted Calls	Indicates the total number of attempted calls on the SIP Trunk Session.
Calls in Progress	Indicates the total number of calls in progress on the SIP Trunk Session.
Completed Calls	Indicates the total number of completed calls on the SIP Trunk Session.

Enabling the Monitoring of SIP Trunk Sessions

The **Monitoring Configuration for UCM Cluster** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of SIP Trunk Sessions. The page displays the list of existing SIP trunk session configuration settings under the **SIP Trunk Sessions** tab along with the attributes enabled and the thresholds set for each configured measurement. However, you can configure the SIP trunk sessions settings only after configuring the SSH credentials for the Cisco Unified Communication Manager that you want to monitor. For more information about configuring SSH credentials, see Accessing the Cisco Unified Communications Manager with SSH.

To enable the monitoring of SIP trunk sessions, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters**. The UCM Clusters view opens.
3. Select a UCM Cluster of your interest and click **Actions** > **IP Telephony** > **Monitoring Configuration**. The **Monitoring Configuration for UCM Cluster** page opens.

   Tip: Alternatively, you can also launch the Monitoring Configuration page for the SIP trunk sessions from the SIP Trunk Details and the Call Controller Details forms. When you launch the page using the SIP Trunk Details and the Call Controller Details forms, you cannot do the following:

   - Add a new SIP trunk sessions monitoring configuration
   - Delete an existing SIP trunk sessions monitoring configuration
   - Enable or disable monitoring

   However, you can add the threshold settings only at the SIP Trunk Details form level.
4. On the left pane of the **Monitoring Configuration for UCM Cluster** page, select **SIP Trunk Sessions** from the **Area of Monitoring** drop-down list.
5. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the SIP Trunk Sessions Settings.

6. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the SIP Trunk Sessions setting, go to **Step 5**.

7. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the SIP Trunk Sessions for the UCM Cluster. The default value is five minutes. You can select only a value that is greater than the default value.

8. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing SIP Trunk Sessions configuration setting, follow these steps:

1. Select the SIP Trunk Sessions configuration that you want to modify, and then click **Edit**. The **Add/Update SIP Trunk Sessions** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing SIP Trunk Sessions configuration setting, follow this step:

- Select the SIP Trunk Sessions configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing SIP Trunk Sessions configuration settings.

To disable an existing SIP Trunk Sessions configuration setting, follow this step:

- Select the SIP Trunk Sessions configuration that you want to disable, and then click **Disable All**.

Note: The **Delete**, **Delete All**, and **Disable All** buttons are enabled only at the **UCM Cluster** level.

Configuring the SIP Trunk Sessions Settings

The **Add/Update SIP Trunk Sessions** page enables you to define the attributes for configuring SIP Trunk Sessions.

To configure SIP Trunk Sessions settings, follow these steps:

1. On the **Add/Update SIP Trunk Sessions** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the SIP Trunk Sessions type that is to be monitored. You can select one of the following types of measurement: ▪ **Active Calls** ▪ **Attempted Calls** ▪ **Calls in Progress** ▪ **Completed Calls** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** check box to enable collection for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the SIP Trunk Sessions type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.

Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the SIP Trunk Sessions type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Monitoring RAID Status

You can configure the NNM iSPI for IP Telephony to monitor the status of the various attributes of the Redundant Array of Independent Disks (RAID) of a Cisco Unified Communications Manager (CUCM). You can monitor the following activities:

RAID Status	Description
Critical Disks	Indicates the total number of critical disks on the RAID of the CUCM.
Disks	Indicates the total number of disks on the RAID of the CUCM.
Failed Disks	Indicates the total number of failed disks on the RAID of the CUCM.
Media Error Count	Indicates the total number of media errors on all the slots of the RAID.
Other Error Count	Indicates the total number of other errors on all the slots of the RAID.
Physical Devices	Indicates the total number of physical devices on the RAID of the CUCM.

Enabling the Monitoring of RAID Status

The **Monitoring Configuration for UCM Cluster** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of RAID status. The page displays the list of existing RAID status configuration settings under the **RAID Status** tab, along with the attributes enabled and the thresholds set for each configured measurement. However, you can configure the RAID status settings only after configuring the SSH credentials for the Cisco Unified Communication Manager that you want to monitor. For more information about configuring SSH credentials, see Accessing the Cisco Unified Communications Manager with SSH.

To enable the monitoring of RAID status, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters**. The UCM Clusters view opens.
3. Select the cluster for which you want to launch the **Cisco Call Controller Details** form, and then click . The UCM Cluster Details form opens.
4. On the right pane of the form click the **UCMs** tab. The UCMs view opens.
5. From the list of UCMs, select the Cisco Unified Communications Manager for which you want to enable the monitoring of the RAID status, and then click . The **Cisco Call Controller Details** form opens.
6. Click **Actions** > **IP Telephony** > **Monitoring Configuration**. The **Monitoring Configuration for UCM** page opens.
7. On the left pane of the **Monitoring Configuration for UCM Cluster** page, select **RAID Status** from the **Area of Monitoring** drop-down list.
8. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the RAID Status Settings.
9. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the RAID Status setting, go to **Step 8**.
10. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to periodically monitor the RAID Status for the UCM Cluster. The default value is five minutes. You can select only a value that is greater than the default value.
11. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing RAID Status configuration setting, follow these steps:

1. Select the RAID Status configuration that you want to modify, and then click **Edit**. The **Add/Update RAID Status** page opens.
2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing RAID Status configuration setting, follow this step:

- Select the RAID Status configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing RAID Status configuration settings.

To disable an existing RAID Status configuration setting, follow this step:

- Select the RAID Status configuration that you want to disable, and then click **Disable All**.

Configuring the RAID Status Settings

The **Add/Update RAID Status** page enables you to define the attributes for configuring RAID Status.

To configure RAID Status settings, follow these steps:

1. On the **Add/Update RAID Status** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the RAID Status type that is to be monitored. You can select one of the following types of measurement: ▪ **Critical Disks** ▪ **Disks** ▪ **Failed Disks** ▪ **Media Error Count** ▪ **Other Error Count** ▪ **Physical Devices** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type. **Note:** You cannot configure values for the threshold violation of the **Disks** and **Physical Devices** measurement types.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting for the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the RAID status type threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the RAID status type threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the configuration settings.

Monitoring the Cisco TFTP Server

You can configure the NNM iSPI for IP Telephony to monitor the configuration file builds performed by the Cisco TFTP server for a UCM. You can monitor the following activities:

Configuration File Build Activity	Description
BuildAbortCount	Indicates the number of times the configuration file build process was aborted. The count increases when the build process for devices, soft keys, units, and dial rules get aborted due to group-level change notifications.
BuildCount	Indicates the number of times the TFTP server performed a new build of all the configuration files in response to a database change notification affecting all the devices. The count starts from the time the TFTP service started.
BuildDeviceCount	Indicates the number of devices that were processed during the last configuration build. This count increases when processing device change notifications. The count increases when new devices get added and reduces when existing devices are removed.
BuildDialRuleCount	Indicates the number of dial rules that were processed during the last configuration build. This count increases when processing dial rule change notifications. The count increases when new dial rules get added and reduces when existing dial rules are removed.
BuildSignCount	Indicates the number of security-enabled phones for which the configuration file was digitally signed with the Cisco UCM server key during the last configuration build. The count increases when processing security-enabled phone change notifications.
BuildSoftKeyCount	Indicates the number of soft keys that were processed during the last configuration build. The count increases when new soft keys get added and reduces when existing soft keys are removed.
BuildUnitCount	Indicates the number of gateways that were processed during the last configuration build. The count increases when processing gateway change notifications. The count increases when new gateways get added and reduces when existing gateways are removed.
ChangeNotifications	Indicates the total number of all the Cisco UCM database change notifications received by the TFTP server. This count increases every time a device configuration is updated using the Cisco UCM Administration interface. This update triggers a database change notification to the TFTP server to rebuild the configuration files.
DeviceChangeNotifications	Indicates the number of times the TFTP server received database change notifications to create, update, or delete configuration files for devices.

DialRuleChangeNotifications	Indicates the number of times the TFTP server received database change notifications to create, update, or delete configuration files for dial rules.
HTTPRequestsAborted	Indicates the total number of HTTP requests canceled by the HTTP server unexpectedly. An HTTP request cancellation occurs when the requested device cannot be located on the network or when the file transfer gets interrupted due to network connectivity issues.
HTTPRequestsProcessed	Indicates the total number of HTTP requests successfully processed by the HTTP server.
RequestsAborted	Indicates the total number of TFTP requests canceled by the TFTP server unexpectedly. A TFTP request cancellation occurs when the requested device cannot be located on the network or when the file transfer gets interrupted due to network connectivity issues.
RequestsProcessed	Indicates the total number of TFTP requests successfully processed by the TFTP server.

Enabling the Monitoring of Cisco TFTP Server

The **Monitoring Configuration for UCM** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the TFTP server activity. The page displays the list of existing TFTP server activity configuration settings under the **Cisco TFTP Server** tab along with the attributes enabled and the thresholds set for each configured measurement. However, you can configure the TFTP Server activity settings only after configuring the SSH credentials for the Cisco Unified Communication Manager that you want to monitor. For more information about configuring SSH credentials, see Configuring SSH Access for a Cisco Unified Communications Manager Cluster.

You can launch the **Monitoring Configuration for UCM** page from the **Cisco Call Controller Details** form of a UCM.

To enable the monitoring of Cisco TFTP server, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters**. The UCM Clusters view opens.
3. Select the cluster for which you want to launch the **Cisco Call Controller Details** form, and then click . The UCM Cluster Details form opens.
4. On the right pane of the form click the **UCMs** tab. The UCMs view opens.
5. From the list of UCMs, select the Cisco Unified Communications Manager for which you want to enable the TFTP server monitoring, and then click . The **Cisco Call Controller Details** form opens.

6. Click **Actions** > **IP Telephony** > **Monitoring Configuration**. The **Monitoring Configuration for UCM** page opens.

7. On the left pane of the **Monitoring Configuration for UCM** page, select **Cisco TFTP Server** from the **Area of Monitoring** drop-down list.

8. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the Cisco TFTP Server Settings.

9. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the TFTP Server setting, go to **Step 8**.

10. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to monitor the configuration file build activities performed by the Cisco TFTP server periodically.

11. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing TFTP Server configuration setting, follow these steps:

1. Select the TFTP Server activity configuration that you want to modify, and then click **Edit**. The **Add/Update Cisco TFTP Server** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing TFTP Server configuration setting, follow this step:

- Select the TFTP Server activity configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing TFTP Server activity configuration settings.

To disable an existing TFTP Server configuration setting, follow this step:

- Select the TFTP Server activity configuration that you want to disable, and then click **Disable All**.

Configuring the Cisco TFTP Server Settings

The **Add/Update Cisco TFTP Server** page enables you to define the attributes for configuring the Cisco TFTP server settings such as specifying threshold settings to generate incidents based on the TFTP server activity, and enable monitoring and reporting for the TFTP server activity.

To configure the Cisco TFTP Server settings, follow these steps:

1. On the **Add/Update Cisco TFTP Server** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the TFTP Server type activity that is to be monitored. You can select one of the following types of measurement: ▪ **RequestsProcessed** ▪ **BuildAbortCount** ▪ **BuildCount** ▪ **BuildDeviceCount** ▪ **BuildDialRuleCount** ▪ **BuildSignCount** ▪ **BuildSoftKeyCount** ▪ **BuildUnitCount** ▪ **ChangeNotifications** ▪ **DeviceChangeNotifications** ▪ **DialRuleChangeNotifications** ▪ **HTTPRequestsAborted** ▪ **HTTPRequestsProcessed** ▪ **RequestsAborted** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting of the selected Measurement Type.

Generate Incident	Select the check box to generate incident in the incident inventory.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the selected TFTP Server threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the TFTP Server threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the TFTP Server activity configuration settings.

Monitoring the Health of Cisco Unified Communications Managers

You can configure the NNM iSPI for IP Telephony to monitor the UCM parameters that indicate the health of the system. You can monitor the following activities:

System Health Parameter	Description
Active Partition Used	Indicates the total space in use by the active partition.
Common Partition Used	Indicates the total space in use by the common partition.
CPU Time	Indicates the CPU utilization of the Cisco Unified Communications Manager.
Memory Used	Indicates the memory utilization of the Cisco Unified Communications Manager.
Process: ccm - CPU Time	Indicates the CPU utilization of the `ccm` process.
Process: ccm - Memory Used	Indicates the memory utilization of the `ccm` process.
Swap Partition Used	Indicates the total space in use by the swap partition.
Swap Space Used	Indicates the total swap space used by the Cisco Unified Communications Manager.
System Reboot	Indicates whether there was a reboot during the last polling cycle.
System Uptime	Indicates the time elapsed since the last reboot.
Total Processes	Indicates the total number of processes on the Cisco Unified Communications Manager.
Total Threads	Indicates the total number of threads on the Cisco Unified Communications Manager.
VM Used	Indicates the total virtual memory in use.

Enabling the Monitoring of System Health Parameters

The **Monitoring Configuration for UCM** page enables you to configure monitoring of system health parameters of Cisco Unified Communications Managers.

To enable the monitoring of system health parameters, follow these steps:

1. Log on to the NNMi console as an administrator.
2. Navigate to the **Monitoring Configuration for UCM** page.
   a. From the NNMi workspace, click **Cisco IP Telephony > UCM Clusters**. The UCM Clusters view opens.
   b. Select the cluster for which you want to launch the **Cisco Call Controller Details** form, and then click . The UCM Cluster Details form opens.
   c. On the right pane of the form click the **UCMs** tab. The UCMs view opens.
   d. From the list of UCMs, select the Cisco Unified Communications Manager for which you want to enable the system health parameter monitoring, and then click . The **Cisco Call Controller Details** form opens.
   e. In the Cisco Call Controller Details form, click **Actions > IP Telephony > Monitoring Configuration**. The **Monitoring Configuration for UCM** page opens.
3. On the left pane of the **Monitoring Configuration for UCM** page, select **System Health** from the **Area of Monitoring** drop-down list.
4. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the System Health Parameter Settings.
5. Click (the **Refresh** icon) to view the newly-added measurement type. To add more measurement types to the System health Parameter setting, go to **Step 4**.
6. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to monitor the system health parameters periodically.
7. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing System Health parameter configuration setting, follow these steps:

1. Select the System Health parameter configuration that you want to modify, and then click **Edit**. The **Add/Update System Health** page opens.
2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing System Health parameter configuration setting, follow this step:

- Select the System Health parameter configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing System Health parameter configuration settings.

To disable an existing System Health parameter configuration setting, follow this step:

- Select the System Health parameter configuration that you want to disable, and then click **Disable All**.

Configuring the System Health Parameter Settings

The **Add/Update System Health** page enables you to define the attributes for configuring the system health parameters such as specifying threshold settings to generate incidents, and enable monitoring and reporting for the system health.

To configure the system health parameters settings, follow these steps:

1. On the **Add/Update System Health** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Measurement Type	Indicates the System Health parameter type that is to be monitored. You can select one of the following types of measurement: ▪ **Active Partition Used** ▪ **Common Partition Used** ▪ **CPU Time** ▪ **Memory Used** ▪ **Process: ccm - CPU Time** ▪ **Process: ccm - Memory Used** ▪ **Swap Partition Used** ▪ **Swap Space Used** ▪ **System Reboot** ▪ **System Uptime** ▪ **Total Processes** ▪ **Total Threads** ▪ **VM Used** **Note:** The **Measurement Type** list also provides the **All** option that enables you to select the **Enable Collection** and **Enable Reporting** check boxes to enable collection and reporting respectively, for all the available measurement types for this category. However, you must not configure any thresholds if you have selected **All**, as the threshold value for measurement types vary. You must always set the threshold values separately for each measurement type.
Enable Collection	Select the check box to enable collection of the selected Measurement Type.
Enable Reporting	Select the check box to enable reporting of the selected Measurement Type.
Generate Incident	Select the check box to generate incident in the incident inventory.

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ■ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ■ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ■ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ■ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Lower Base	Specify the lower base value for the selected System Health parameter threshold.
% Lower Deviation	Specify the acceptable percentage of deviation from the lower base threshold value before generating an incident.
Abs Lower Deviation	Specify the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
Lower Trigger Count	Specify the number of times the threshold deviation should be permitted for the lower base before generating the incident. Specifying the trigger count is mandatory for generating incidents.
Higher Base	Specify the higher base value for the System Health parameter threshold.
% Higher Deviation	Specify the acceptable percentage of deviation from the higher base threshold value before generating an incident.
Abs Higher Deviation	Specify the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
Higher Trigger Count	Specify the number of times the threshold deviation should be permitted for the higher base before generating the incident. Specifying the trigger count is mandatory for generating incidents.

2. Click (the **Save** icon) to save the System Health parameter configuration settings.

Monitoring the Availability of the Call Manager Administration Web Page

You can configure the NNM iSPI for IP Telephony to monitor the following activity:

- CCMAdmin Web Page: Indicates the availability of the administration web page for a Cisco Unified Communications Manager

Enabling the Monitoring of the Call Manager Administration Web Page State

The **Monitoring Configuration for UCM** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the availability of the administration web page for a CUCM. The page displays the list of existing administration web page state configuration settings under the **Availability** tab along with the attributes enabled and the thresholds set for each configured measurement.

To enable the monitoring of the administration web page state for a CUCM, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters**. The UCM Clusters view opens.
3. Select the cluster for which you want to launch the **Cisco Call Controller Details** form, and then click . The UCM Cluster Details form opens.
4. On the right pane of the form click the **UCMs** tab. The UCMs view opens.
5. From the list of UCMs, select the Cisco Unified Communications Manager for which you want to enable the monitoring of the administration web page state for the CUCM, and then click . The **Cisco Call Controller Details** form opens.
6. Click **Actions** > **IP Telephony** > **Monitoring Configuration**. The **Monitoring Configuration for UCM** page opens.
7. On the left pane of the **Monitoring Configuration for UCM** page, select **Availability** from the **Area of Monitoring** drop-down list.
8. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the Call Manager Administration Web Page State Settings.
9. Click (the **Refresh** icon) to view the newly-added measurement type.
10. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony

uses this value to monitor the availability of the administration web page for the CUCM periodically.

11. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing call manager administration web page state configuration setting, follow these steps:

1. Select the call manager administration web page state configuration that you want to modify, and then click **Edit**. The **Add/Update Availability** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing call manager administration web page state configuration setting, follow this step:

- Select the call manager administration web page state configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing call manager administration web page state configuration settings.

To disable an existing call manager administration web page state configuration setting, follow this step:

- Select the call manager administration web page state configuration that you want to disable, and then click **Disable All**.

Configuring the Call Manager Administration Web Page State Settings

The **Add/Update Availability** page enables you to define the attributes for the availability of the administration web page for a CUCM, such as specifying threshold settings to generate incidents, and enable monitoring for the availability.

To configure the availability of the administration web page for a CUCM settings, follow these steps:

1. On the **Add/Update Availability** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the Availability type that is to be monitored. The following measurement type is available: ▪ **CCMAdmin Web Page**
Enable Collection	Select the check box to enable collection of the availability of administration web page for the call manager.

Generate Incident	Select the check box to generate incident in the incident inventory.
Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.
Threshold State	Select one of the following options to specify the threshold state: ▪ **Available**: Indicates the administration web page for the call manager is available. ▪ **Not Available**: Indicates the administration web page for the call manager is not available.

2. Click (the **Save** icon) to save the call manager administration web page state configuration settings.

Monitoring the Availability of Services on the UCM

You can configure the NNM iSPI for IP Telephony to monitor the availability of the services on a UCM. You can configure the NNM iSPI for IP Telephony to generate incidents based on the state of the services. You can configure the NNM iSPI for IP Telephony to generate incidents if the state of the service changes from `Started` to `Stopped`, or `Deactivated` or in the reverse scenarios.

Note: The NNM iSPI for IP Telephony allows you to monitor the availability of the services currently on the discovered UCM.

Enabling the Monitoring of the Availability of Services on the UCM

The **Monitoring Configuration for UCM** page of the NNM iSPI for IP Telephony helps you to enable the monitoring of the state of the services on a UCM. The page displays the list of existing configuration settings under the **Services** tab along with the attributes enabled and the thresholds set for each configured measurement. However, you can configure the state of available services settings only after configuring the SSH credentials for the Cisco Unified Communication Manager that you want to monitor. For more information about configuring SSH credentials, see Configuring SSH Access for a Cisco Unified Communications Manager Cluster.

Note: After configuring the SSH credentials, you must perform a discovery on the CUCM node for all the measurements to be displayed in the **Measurement Type** list.

To enable the monitoring of the availability of the services, follow these steps:

1. From the NNMi console, click the **Cisco IP Telephony** workspace in the left pane.
2. Click **UCM Clusters**. The UCM Clusters view opens.
3. Select the cluster for which you want to launch the **Cisco Call Controller Details** form, and then click . The UCM Cluster Details form opens.
4. On the right pane of the form click the **UCMs** tab. The UCMs view opens.
5. From the list of UCMs, select the Cisco Unified Communications Manager for which you want to enable the monitoring of the availability of services, and then click . The **Cisco Call Controller Details** form opens.
6. Click **Actions** > **IP Telephony** > **Monitoring Configuration**. The **Monitoring Configuration for UCM** page opens.
7. On the left pane of the **Monitoring Configuration for UCM** page, select **Services** from the **Area of Monitoring** drop-down list.
8. From the right pane of the page, click (the **New** icon) to add the Measurement Type. For more information about adding a Measurement Type, see Configuring the Availability of Services on the UCM Settings.
9. Click (the **Refresh** icon) to view the newly-added measurement type.
10. On the left pane of the page, select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The NNM iSPI for IP Telephony uses this value to monitor the state of the services on a UCM periodically.
11. Click (the **Save** icon) to save the monitoring configuration.

To modify an existing availability of Services setting, follow these steps:

1. Select the Service Availability configuration that you want to modify, and then click **Edit**. The **Add/Update UCOS Service Availability** page opens.

2. Make the required changes and click (the **Save** icon) to save the modified configuration settings.

To delete an existing availability of Services setting, follow this step:

- Select the Service Availability configuration that you want to delete, and then click **Delete**. You can click **Delete All** to delete all the existing Service Availability configuration settings.

To disable an existing availability of Services setting, follow this step:

- Select the Service Availability configuration that you want to disable, and then click **Disable All**.

Configuring the Availability of Services on the UCM Settings

The **Add/Update UCOS Service Availability** page enables you to define the attributes to monitor the service availability settings such as specifying threshold settings to generate incidents, enabling monitoring for service state changes, and enabling reporting for service availability and service state changes.

To configure the service availability settings, follow these steps:

1. On the **Add/Update UCOS Service Availability** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Measurement Type	Indicates the Services that are to be monitored.
Enable Collection	Select the check box to enable collection of the services.
Generate Incident	Select the check box to generate incident in the incident inventory.
State	Select one of the following options to specify the state: ▪ **Started** ▪ **Stopped** ▪ **De-Activated**

Threshold Severity	Indicates the severity of the incident that is generated during a threshold violation. You can select one of the following types: ▪ **Critical**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachCrirtical*) incident. ▪ **Major**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMajor*) incident. ▪ **Minor**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachMinor*) incident. ▪ **Warning**: The NNM iSPI for IP Telephony generates a (*MonitoredAttributeThresholdBreachWarning*) incident. **Note:** The NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents.

2. Click (the **Save** icon) to save the service availability configuration settings.

ClarusIPC Integration–Test Plans and Test Result Reports

The integration of NNM iSPI for IP Telephony with ClarusIPC presents the following additional workspaces for Cisco IP Telephony:

- Test Plans: provides a list of ClarusIPC test plans configured.
- Test Result Reports: provides reports of the ClarusIPC automated test results.

In addition, this integration helps you launch the ClarusIPC **Remote Hands** and **Help Desk** views from the NNMi console.

To launch ClarusIPC Remote Hands, go to the Cisco IP Phones view, select an IP phone, and then click **Actions > Remote Hands**.

To launch ClarusIPC Help Desk, go to the Cisco IP Phones view, select an IP phone, and then click **Actions > Help Desk**.

To enable the integration with ClarusIPC, see Integrate the NNM iSPI for IP Telephony with ClarusIPC.

Viewing Route Group P.01 Grade of Service Summary Report

This report lets you do call routing capacity planning by generating the usage summary of Cisco Route Groups configured on Cisco Call Manager clusters. This report is applicable only for the Route Groups that reference channelized Cisco Voice Gateways or channelized Cisco Voice Gateway interfaces such as T1/E1 PRIs. This report captures a summary of the usage for any Route Group as a logical bundle of channels along with the summary of usage for each gateway device referenced by the Route Group.

The report displays the final result for the group and each gateway in the group and also includes an indicator of the Grade of Service for the set as well as for each Gateway device in the set. This indicator indicates a percent of P.01 Grade Of Service for the number of channels in the set of Gateways for the group. the report displays the compliance indicator for each Gateway device in the selected group.

P.01 Grade of Service indicates, for a given number of channels in a logical bundle, the Busy Hour Traffic (BHT) that the set representing the logical bundle can sustain with a 0.01% blockage.

The report uses hourly aggregated Cisco CDR reported call information stored in NPS under Cisco IP Telephony Gateway Calls reporting package to arrive at the conclusions.

For each gateway device in the set, the report first determines the Total calls, the Average Duration for a call and the Busiest Day Calls carried by the gateway in the selected time period. The report then estimates the Busiest Hour Calls offered to the gateway by calculating a fraction of Busiest Day Calls. The report uses a fractional multiplier of 14% by default. You can configure this multiplier before generating the report. After estimating the Busiest Hour Calls offered, the report estimates the Busiest Hour Traffic (BHT) by calculating the Busiest Hour Calls offered multiplied by the Average Duration for a Call. The report then compares the BHT against the P.01 GoS BHT for the number of channels in the gateway device and displays the comparison as a percentage and indicates the compliance to P.01 GoS Standards.

The report performs similar calculations for the Route Group as a set of gateways and therefore treats the set of gateways as a logical bundle of channels. The report first determines the Total Calls, the Average Duration for a call, and the Busiest Day Calls carried for the complete set of gateways referenced by the Route Group. The Average Duration for a call and the Busiest Day Calls carried are for the set of gateways and is not the sum of the same parameters for all the gateways. The report then estimates the Busiest Hour Calls offered for the Route Group by calculating a fraction of Busiest Day Calls carried for the same. The report uses a fractional multiplier of 14% by default. You can configure this multiplier before generating the report. After estimating the Busiest Hour Calls offered, the report estimates the Busiest Hour Traffic (BHT) by calculating the Busiest Hour Calls offered multiplied by the Average Duration for a Call. The report then compares the BHT against the P.01 GoS BHT for the number of channels in the gateway device and displays the comparison as a percentage and indicates the compliance to P.01 GoS Standards. The total number of channels for a Route Group is the sum of the number channels for all the gateways referenced by the Route Group.

- You must configure Cisco AXL Data access configuration as specified in the "Configuring Data Access " on page 476 section before viewing this report.
- You must configure Cisco CDR access configuration as specified in the "Configuring Data Access " on page 476 section before viewing this report.
- You must enable CDR-based reporting as specified in the "Configure Reporting" on page 497 section before viewing this report.

To access the Route Group P.01 GoS Summary Report:

1. Log on to the NNMi console as an operator.
2. Click **Cisco IP Telephony > UCM Clusters**.
3. Select a Cisco Unified Communications Manager cluster of your choice, and then click **Actions > IP Telephony > Route Group P.01 GoS Summary**. The Grade of Service for Route Group window opens.
4. Specify the following details on the left panel:
   - **Fraction***: Specify the numeric value that denotes the percentage of busiest day calls to be taken as the estimated busy hour calls offered. The default value is 14 for this parameter.
   - **Start Date**: Specify the start date for the report.
   - **End Date**: Specify the end date for the report.

     Note: HP recommends that you provide a gap of a day or more between the start date and the end date to generate reports, By default, the NNM iSPI for IP Telephony generates the report for the past one week.

   - **Direction**: Select one of the following options to specify the type pf calls that must be considered when generating reports.
     - In: indicates incoming calls.
     - Out: indicates outgoing calls.
     - Both: indicates both incoming and outgoing calls.
   - **Time Zone**: Select the time zone configured in your system. You must select the Default time zone if NNMi and the iSPI Performance for Metrics are installed on different time zones.
   - **Cluster ID**: Specifies the cluster identifier.
   - **Route Groups**: Select the route groups based on which you want to monitor the usage of the gateways and calculate the P.01 GoS score.

5. Click **Submit**. The report for the selected Cisco Unified Communications Manager cluster opens.

The **Selection Order** in the report indicates the priority or position of the gateway device within a Route Group.

Note: The **GOS Reference Chart** lists the number of channels and the recommended GoS score for the respective number of channels.

Viewing Route List P.01 Grade of Service Summary Report

This report helps you to do call routing capacity planning by generating the usage summary of all Cisco Route Groups referenced by specific selected Route Lists configured on Call Manager clusters.

This report is applicable only for the Route Lists that has at least one Route Group referencing channelized Cisco Voice Gateways or channelized Cisco Voice Gateway interfaces such as T1/E1 PRIs. This report captures a summary of the usage for each Route Group referenced by each Route List. The report displays the summary for each Route Group referenced by the Route Lists where the summary for each Route Group represents the summary similar to what you can generate for that Route Group from the Cisco Route Group P.01 GoS Summary tool. For more information on Cisco Route Group P.01 GoS Summary, see "Viewing Route Group P.01 Grade of Service Summary Report" on page 310

- You must configure Cisco AXL Data access configuration as specified in the "Configuring Data Access " on page 476 section before viewing this report.
- You must configure Cisco CDR access configuration as specified in the "Configuring Data Access " on page 476 section before viewing this report.
- You must enable CDR-based reporting as specified in the "Configure Reporting" on page 497 section before viewing this report.

To access the Route List P.01 GoS Summary Report:

1. Log on to the NNMi console as an operator.
2. Click **Cisco IP Telephony > UCM Clusters**.
3. Select a Cisco Unified Communications Manager cluster of your choice, and then click **Actions > IP Telephony > Route List P.01 GoS Summary**. The Grade of Service for Route List window opens.

4. Specify the following details on the left panel:
   - **Fraction***: Specify the numeric value that denotes the percentage of busiest day calls to be taken as the estimated busy hour calls offered. The default value is 14 for this parameter.
   - **Start Date**: Specify the start date for the report.
   - **End Date**: Specify the end date for the report.

     Note: HP recommends that you provide a gap of a day or more between the start date and the end date to generate reports. By default, the NNM iSPI for IP Telephony generates the report for the past one week.

   - **Direction**: Select one of the following options to specify the type pf calls that must be considered when generating reports.
     - In: indicates incoming calls.
     - Out: indicates outgoing calls.
     - Both: indicates both incoming and outgoing calls.
   - **Time Zone**: Select the time zone configured in your system. You must select the Default time zone if NNMi and the iSPI Performance for Metrics are installed on different time zones.
   - **Cluster ID**: Specifies the cluster identifier.
   - **Route List**: select the route lists based on which you want to monitor the usage of the route groups and calculate the P.01 GoS score.
5. Click **Submit**. This generates the report.

Note: The Route Lists reference the gateway devices through references to the Route Groups. The Route Groups reference the Gateway devices. In order to see the detailed summary for each gateway in a given Route Group, you can filter the detailed Gateway Summary table by entering the name of the Route Group noted from the Route Groups Summary table for any Route List.

The **Selection Order** in the report indicates the priority or position of the Route Group within a given Route List.

Note: The **GOS Reference Chart** lists the number of channels and the recommended GoS score for the number of channels.

Microsoft IP Telephony

You can monitor the Microsoft IP telephony network by logging in as an operator (level 1 or level 2) or as a guest. After logging in, you can view the inventory views for the different Microsoft IP telephony devices and entities discovered and monitored. The following table lists the options that you can click to view the details of a discovered device or an entity:

Inventory View	Purpose
Lync Sites	Lists the Lync sites discovered on the network.
End User Groups	Lists the end user groups discovered on the network for the Lync Server.
Lync End Users	Lists the end users discovered on the network for the Lync Server.
Servers	Lists the servers discovered from all the server pools associated with the Lync server on the network.
Gateways	Lists the gateways discovered on the network.
SIP Trunks	Lists the SIP trunks discovered on the network.
Dial Plans	Lists the dial plans discovered on the network.
Voice Routes	Lists the voice routes discovered on the network.
Voice Policies	Lists the voice policies discovered on the network.

Monitoring Lync Sites

You can use the Lync Sites inventory view to see a list of Lync sites discovered on the network.

To access the Lync Sites inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest.
2. Click **Microsoft IP Telephony**. The inventory options that you can click to view the inventory view for that device or entity, appear.
3. Click **Lync Sites**. The Lync Sites inventory view appears.

The Lync Sites inventory view displays the list of Lync sites discovered on the network along with the following attributes for each Lync site.

Attribute	Description
Identity	Indicates the unique identity of the Lync site discovered.
Name	Indicates the name of the Lync site discovered.
Type	Indicates the type of the Lync site discovered. The type can be one of the following: • Remote Site: indicates that the discovered site is a remote site managed by a central site. • Central Site: indicates that the discovered site is a central site that manages remote sites.
Parent Site	Indicates the identity of the site that manages the remote site. This field is applicable only for remote sites.
Description	Indicates the description configured for the Lync site discovered..
Management Server	Indicates if the Lync site is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the Lync sites discovered: • Local: If the Lync site is being managed by the NNMi management server console on which you are viewing the IP phone details. • Name of the regional manager that manages the Lync site.

You can view additional details for a discovered Lync site using the Lync site form.

Viewing the Analysis Panel for a Quick Reference

The Analysis panel that appears at the bottom of the Lync Sites inventory view displays the following details. You can select a Lync Site from the Lync Sites inventory view to automatically launch the Analysis panel:

- Left panel: This panel displays the summary for the selected Lync site and displays the following details:

Detail	Description
No. of Branches	The number of branch sites connected to the selected Lync site.
No. of Gateways	The number of gateways discovered in the selected Lync site.
No. of Pools	The number of server pools discovered in the selected Lync site.

Detail	Description
No. of Users	The number of users discovered in the selected Lync site.
Parent Site	The name of the parent site associated with the selected Lync site.
Primary Registrar Pool	The primary registrar pool associated with the selected Lync site.
Backup Registrar Pool	The backup registrar pool associated with the selected Lync site.
Last Discovered	The date and time during which the Lync site was last discovered.

- Right panel: The right panel displays pie charts for the following call analysis details:
  - QoE by calling party
  - QoE for called party
  - Calls by Media Type
  - Calls by Call Type
  - Calls by Session Type
  - Top Callers
  - Top Named Callers

Launching Context-sensitive Actions for a Lync Site

You can perform the following context-sensitive actions for a selected Lync site from the Lync Sites inventory view:

- Launch the call details chart detail report.
- Launch the call quality chart details report.
- Discover topology and discover users.

To launch the context-sensitive actions, do as follows:

1. Select the Lync site
2. Click **Actions** > **Microsoft IP Telephony**and select the appropriate option to launch the required action.

Note: The pie charts display the details for the past 24 hours. You can click the (Refresh) icon to display the pie chart with the latest call analysis details.

Lync Sites Form

You can use the Lync Sites form to view additional details about a discovered Lync site.

To access the Lync Sites form, follow these steps:

1. Select a Lync site discovered from the Lync Sites inventory view.
2. Click (**Open**). The Lync Sites form opens.

The Lync Sites form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Tab	Description
Identity	Indicates the unique identity of the Lync site discovered.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**

This tab displays the general site attributes as follows.

Attribute	Description
Name	Indicates the name of the site.
Type	Indicates the type of the site. The type can be one of the following: • Remote Site: indicates that the discovered site is a remote site managed by a central site. • Central Site: indicates that the discovered site is a central site that manages remote sites.
Parent Site	Indicates the identity of the site that manages the remote site. This field is applicable only for remote sites.
Primary Registrar Pool	Indicates the name of the primary registrar pool for the site.
Backup Registrar Pool	Indicates the name of the backup registrar pool for the site.
Description	Indicates the description for the site.

- **Pools**

This tab displays the server pools associated with the Lync site as follows

Attribute	Description
Identity	The identity of the server pool associated with the Lync site.
FQDN	The Fully Qualified Domain Name (FQDN) of the server pool.

Select a server pool and click (**Open**). This opens the Pool form.

- **Gateways**: displays the gateways associated with the Lync site as shown in the Gateways inventory view.
- **SIP Trunks**: displays the SIP trunks associated with the Lync site as shown in the SIP Trunk Configuration form.

Pool Form

You can use the Pool form to view additional details about a discovered server pool associated with a Lync site.

To access the Pools form, do as follows:

1. Select a pool associated with a Lync site from the Pools tab page on the Lync Sites form.
2. Click (**Open**). This opens the Pool form.

The Pool form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down list.

Tab	Description
Identity	Indicates the unique identity of the server pool associated with the Lync site.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**: displays the general pool attributes as follows.

Attribute	Description
FQDN	Indicates the Fully Qualified Domain Name (FQDN) of the server pool.

- **Servers**: displays the servers discovered from all the server pools associated with the Lync site. The Servers tab page displays the following attributes.

Attribute	Description
Identity	The unique identity configured for the server.
FQDN	The FQDN of the server.

Select a server and click (**Open** to open the Servers form to see the additional details for a discovered server.

Monitoring End User Groups

You can use the End User Groups inventory view to see a list of end user groups configured on the network.

To access the End User Groups inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest.
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **End User Groups**. The End User Groups inventory view appears.

The End User Groups inventory view displays the list of end user groups discovered on the network along with the following attributes for each end user group.

Attribute	Description
Group Name	Indicates the name of the end user group discovered.
Description	Indicates the description of the end user group discovered.
Order	Indicates the order number for the end user group.
Number of Members	Indicates the number of end users in the group.

You can view additional details for a discovered end user group using the End User Group form.

Viewing the Analysis Panel for a Quick Reference

The Analysis panel that appears at the bottom of the End User Groups inventory view displays the following details. You can select an end user group from the End User Groups inventory view to automatically launch the Analysis panel:

- Left panel: This panel displays the summary for the selected end user group and displays the following details:

Detail	Description
No. of Members	The number of members in the discovered end user group.
Created on	The data and time at which the end user group was .created.
Modified on	The data and time at which the end user group was .modified last.

- Right panel: The right panel displays pie charts for the following call analysis details:
  - QoE by calling party
  - QoE for called party
  - Calls by Media Type
  - Calls by Call Type
  - Calls by Session Type
  - Top Callers
  - Top Named Callers

Note: The pie charts display the details for the past 24 hours. You can click the (Refresh) icon to display the pie chart with the latest call analysis details.

Launching Context-sensitive Actions for a Lync End User Group

You can perform the following context-sensitive actions for a selected Lync end user group from the Lync End User Groups inventory view:

- Launch the call details chart detail report.
- Launch the call quality chart details report.

To launch the context-sensitive actions, do as follows:

1. Select the Lync end user group.
2. Click **Actions** > **Microsoft IP Telephony**and select the appropriate option to launch the required action.

End User Group Form

You can use the End User Group form to view the additional details of an end user group discovered.

To access the End User Group form, do as follows:

1. Select an end user group from the End User Groups inventory view.
2. Click (**Open**). The End User Group form opens.

The End User Group form displays the information in two panels—the left panel and the right panel.

The left panel displays the **Basics** drop-down list that displays the name of the end user group.

The right panel displays the following drop-down lists that display the additional details associated with an end user group.

- General

Attribute	Description
Group Name	Indicates the name of the end user group.
Description	Indicates the description provided while configuring the end user group.
Filter String	Indicates the filter string used to group end users in the end user group.
Order	Indicates the order number configured for the user group

- Lync End Users: displays the details of the end users associated with the selected end user group as shown on the Lync End Users inventory view.

Monitoring End Users

You can use the Lync End Users inventory view to see a list of end users discovered on the network.

To access the Lync End Users inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest.
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Lync End Users**. The Lync End Users inventory view appears.

The Lync End Users inventory view displays the list of end users discovered on the network along with the following attributes for each end user.

Attribute	Description
SIP Address	Indicates the SIP address of the end user.
Display Name	Indicates the display name of the end user.

Attribute	Description
Line URI	Indicates the line URI configured for the end user.
Registrar Pool	Indicates the registrar pool to which the end user is associated.
Named User	Indicates if the end user is configured as a named user. A named user helps in the easy identification of an end user.
Management Server	Indicates if the end user is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the end users discovered: • Local: If the end user is being managed by the NNMi management server console on which you are viewing the IP phone details. • Name of the regional manager that manages the end user.
Lync Site	Indicates the Lync site associated with the end user.

Launching Context-sensitive Actions for a Lync End User

You can perform the following context-sensitive actions for a selected Lync end user from the Lync End Users inventory view:

- Launch the call details chart detail report.
- Launch the call quality chart details report.

To launch the context-sensitive actions, do as follows:

1. Select the Lync end user
2. Click **Actions** > **Microsoft IP Telephony**and select the appropriate option to launch the required action.

You can view additional details for a discovered end users using the Lync End User form.

Lync End User Form

You can use the Lync End User form to view the additional details of an end user discovered.

To access the Lync End User form, do as follows:

1. Select an end user from the Lync End Users inventory view.
2. Click (**Open**). The Lync End User form opens.

The Lync End User form displays the information in two panels—the left panel and the right panel.

The left panel displays the **Basics** drop-down list that displays following attributes of the end user.

Attribute	Description
SIP Address	Indicates the SIP address of the end user.
Display Name	Indicates the display name of the end user.
Line URI	Indicates the line URI configured for the end user.
Registrar Pool	Indicates the registrar pool to which the end user is associated.
Home Server	Indicates the home server to which the end user is associated.

The right panel displays the following drop-down lists that display the additional details associated with an end user group.

- General

Attribute	Description
SIP Address	Indicates the SIP address of the end user.
Display Name	Indicates the display name of the end user.
Line URI	Indicates the line URI configured for the end user.
Registrar Pool	Indicates the registrar pool to which the end user is associated.
Home Server	Indicates the home server to which the end user is associated.
Identity	Indicates the unique identity configured for the end user.
Voice Policy	Indicates the voice policy configured for the end user.
Conferencing Policy	Indicates the conferencing policy configured for the end user.
Dial Plan	Indicates the dial plan configured for the end user.
Location Policy	Indicates the location policy configured for the end user.
Client Policy	Indicates the client policy configured for the end user.
Client Version Policy	Indicates the client version policy configured for the end user.
Archiving Policy	Indicates the archiving policy configured for the end user.
Pin Policy	Indicates the pin policy configured for the end user,
External Access Policy	Indicates the external policy configured for the end user.

Attribute	Description
Hosted Voicemail	Indicates where the voicemail is hosted for the end user.
Hosted Voicemail Policy	Indicates the voice mail policy configured for the end user.
Hosting Provider	Indicates the hosting provider configured for the end user.
Target Registrar Pool	Indicates the target registrar pool configured for the end user.
Target Home Server	Indicates the target home server configured for the end user.
Enabled for Rich Presence	Indicates if the end user is enabled for rich presence. A tick mark in the check box adjacent to this attribute indicates that this attribute is enabled.
Audio Video Disabled	Indicates if audio and video are disabled for the end user. A tick mark in the check box adjacent to this attribute indicates that this attribute is enabled.
Company	Indicates the company name configured for the end user.
Country or Regional Display Name	Indicates the country or regional display name configured for the end user.
Department	Indicates the department configured for the end user.
Country Abbreviation	Indicates the country abbreviation configured for the end user.
City	Indicates the city configured for the end user.
IP Phone	Indicates the IP phone configured for the end user.
Created	Indicates the date and time at which the end user was created
Changed	Indicates the date and time at which the end user configuration was modified last.

- Active Endpoints

Attribute	Description
Client Version	Indicates the client version of the active endpoint associated with the end user.
Pool FQDN	Indicates the Fully Qualified Domain Name (FQDN) of the pool to which the end point belongs.

You can view the additional details regarding an active end point using the Active Endpoints form.

Active Endpoints Form

You can use the Active Endpoint form to view additional details about an active endpoint associated with a Lync end user.

To access the Active Endpoints form, do as follows:

1. Select an active endpoint associated with a Lync end user from the Active Endpoints tab page on the Lync End User form.
2. Click (**Open**). The Active Endpoint form opens.

The Active Endpoint form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Attribute	Description
Client Version	Indicates the client version for the active end point associated with the Lync end user..

The right panel displays the **General** drop-down list that displays the general endpoint attributes as follows.

Attribute	Description
Pool FQDN	The name of the Lync site associated with the SIP trunk.
Edge Server	The edge server associated with the active endpoint.
Manufacturer	The manufacturer for the active endpoint.
Hardware Version	Indicates the hardware version of the active endpoint.

Monitoring Lync Servers

You can use the Servers inventory view to see the servers discovered from all the server pools associated with the Lync server on the network.

To access the Servers inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest.
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Servers**. The Servers inventory view appears.

The Servers inventory view displays the list of servers discovered on the network along with the following attributes for each server:

Attribute	Description
Node Status	Indicates the status of the node.
Identity	Indicates the unique identity of the server discovered.
FQDN	Indicates the Fully Qualified Domain Name (FQDN) of the server.
Pool	Indicates the server pool to which the server belongs.
Management Server	Indicates if the server is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the Lync sites discovered: • Local: If the server is being managed by the NNMi management server console on which you are viewing the server details. • Name of the regional manager that manages the server.
Lync Site	Indicates the Lync site associated with the server.

You can view additional details for a discovered server using the Servers form.

Servers Form

You can use the Servers form to view additional details about a discovered server.

To access the Servers form, do as follows:

1. Select a server discovered from the Servers inventory view.
2. Click (**Open**). The Servers form opens.

The Servers form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Tab	Description
Identity	Indicates the unique identity of the server.
Hosted on Node	Indicates the discovered node that hosts the server.

The right panel displays the following tabs:

- **General**: displays the general site attributes as follows.

Attribute	Description
FQDN	Indicates the name of the site.

Attribute	Description
Pool	Indicates the server pool to which the server belongs.
Management Mode	Indicates if the server is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the Lync sites discovered: • Local: If the server is being managed by the NNMi management server console on which you are viewing the server details. • Name of the regional manager that manages the server.

Monitoring Gateways

You can use the Gateways inventory view to see a list of gateways discovered on the network.

To access the Gateways inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest.
2. Click **Microsoft IP Telephony**.
3. Click **Gateways**. The Gateways inventory view appears.

The Gateways inventory view displays the list of gateways discovered on the network along with the following attributes for each gateway.

Attribute	Description
Node Status	Indicates the status of the NNMi node mapped to the gateway.

Attribute	Description
Operational State	Indicates the operational state of the gateway.This operational state is computed from the operational states of the interfaces contained in the gateway. The operational state for a gateway can display one of the following values: • Minor • Not Applicable • Not Monitored • Unknown • Warning • Normal • Critical • Not Polled
Identity	Indicates the unique identity of the gateway discovered.
Name	Indicates the name of the gateway discovered.
IP Address	Indicates the IP address of the gateway discovered.
Site	Indicates the Lync site that includes the gateway.
Description	Indicates the description configured for the gateway discovered..
Management Server	Indicates if the gateway is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the gateway discovered: • Local: If the gateway is being managed by the NNMi management server console on which you are viewing the gateway details. • Name of the regional manager that manages the gateway.

You can view additional details for a discovered gateway using the Gateway form.

Launching Context-Sensitive Reports for a Gateway

You can launch reports for a gateway from the Gateways inventory view.

To launch the context-sensitive actions, do as follows:

1. Select the gateway.
2. Click **Actions**, select **IP Telephony**, and then click one of the following options:
   - **B-Channel Activity**: Launches Top N Report based on Gateway B-Channel Activity metrics. The default metrics selected are `Gateway Interface Percent Usage (avg)` and `Partially Used Channels (max)`.For more information, see Report online help for Gateway B Channel Activity extension pack.
   - **Call Details**: Launches Top N Report based on Gateway Call Detail metrics. The default metrics selected are `Duration (secs) (avg)` and `Media Type (countDistinct)`. For more information, see Report online help for Call Reports extension pack.
   - **Call Statistics**: Launches Chart Detail Report based on Gateway Statistics metrics. The default metrics selected are `Inbound Calls Blocked (avg)` and `Outbound Calls Blocked (avg)`. For more information, see Report online help for Gateway Statistics extension pack.

Analysis Pane

The Analysis pane displays the following attributes of a selected gateway from the Gateways inventory:

- Version
- Pool FQDN
- Vendor
- Management Mode

See the Gateway form for a description of the listed attributes.

Gateway Form

You can use the Gateway form to view additional details about a discovered gateway.

To access the Gateway form, do as follows:

1. Select a gateway discovered from the Gateways inventory view.
2. Click (**Open**). This opens the Gateway form.

The Gateway form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down list.

Tab	Description
Identity	Indicates the unique identity of the gateway discovered.
Hosted Node	Indicates the discovered node that hosts the gateway.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**: displays the general gateway attributes as follows:

Attribute	Description
Name	Indicates the name of the gateway.
IP Address	Indicates the IP address of the gateway.
Version	Indicates the version of the gateway.
Pool FQDN	Indicates the Fully Qualified Domain Name (FQDN) of the server pool that includes the gateway.
Operational State	The operational state of the gateway. The state can display one of the following values: • Up • Down • Testing • Not Polled • Dormant • Unknown • Not Present • Lower Layer Down • No Polling Policy • Not Monitored • Not Applicable
Site	Indicates the Lync site that includes the gateway.
Vendor	Indicates the vendor name for the gateway.
Description	Indicates the description configured for the gateway.
Management Mode	Indicates whether the gateway is managed or unmanaged.

- **Gateway Interface**: displays the attributes of the gateway interfaces configured with the gateway as follows:

Attribute	Description
Operational State	The operational state of the gateway interface. The state can display one of the following values: • Up • Down • Testing • Not Polled • Dormant • Unknown • Not Present • Lower Layer Down • No Polling Policy • Not Monitored • Not Applicable
Usage State	Indicates the usage state of the gateway interface. The state can be one of the following values: • Idle • Partially Used • Connected
Line Alarmed	Indicates if the gateway interface has active alarms associated during the time of polling. A tick mark indicates the presence of active alarms on the gateway interface.
Name	The name of the gateway interface.
Type	The type of the gateway interface.

Attribute	Description
Administrative State	The administrative state of the gateway interface. The state can display one of the following values: • Up • Down • Testing • Unknown • Not Polled • No Polling Policy • Not Applicable • Not Monitored
Description	The description configured for the gateway interface.

- **Incidents**: Displays the incidents generated for the selected gateway as shown on the incidents page.

The Analysis pane displays a summary of the details of the selected gateway.

You can view the additional details for a gateway interface from the Gateway Interface form.

Gateway Interface Form

You can use the Gateway Interface form to view additional details about the selected gateway interface.

To access the Gateway Interface form, do as follows:

1. Click **Microsoft IP Telephony**.
2. Click **Gateways**. The Gateways inventory view appears.
3. Select a gateway and click (**Open**). The Gateway form opens.
4. Click **Gateway Interface**.Select a gateway interface and click (**Open**). The Gateway Interface form opens.

The Gateway Interface form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down list.

Tab	Description
Name	Indicates the name of the gateway interface.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**: displays the general gateway interface attributes as follows.

Attribute	Description
Index	Indicates the index number configured for the gateway interface.
Type	Indicates the type of the gateway interface.
Speed	Indicates the speed of the gateway interface.
Physical Address	Indicates the physical address of the gateway interface.
Shelf	Indicates the shelf location configured for the gateway interface.
Slot	Indicates the slot configured for the gateway interface.
Port	Indicates the port number configured for the gateway interface.
Channel Number	Indicates the channel number configured for the gateway interface.
Active Line Alarms(s)	Displays the line alarms for the gateway interface as a comma (,) separated list.
Description	Indicates the description configured for the gateway interface.
Last Change	Indicates the time duration from the last time the management server was started to the time the operational state was changed to the current state for the selected gateway interface.

- **Gateway Channel**: displays the gateway channels associated with the gateway interface as follows

Attribute	Description
Operational State	The operational state of the gateway interface. The state can be one of the following values: • Up • Down • Not Polled

Attribute	Description
Usage State	Indicates the usage state of the gateway interface. The state can be one of the following values: • Idle • Partially Used • Connected
Name	The name configured for the gateway channel.
Type	The type of the gateway channel.
Description	The description configured for the gateway channel.

- **Incidents**: Displays the incidents generated for the gateway interfaces discovered on the network as shown on the incidents page.

You can view additional details regarding the gateway channels using the Gateway Channel form.

The Analysis pane at the bottom of the page displays a summary of the attributes of the gateway channel selected:

- Speed: Indicates the speed of the selected gateway interface.
- Physical Address: Indicates the physical address of the selected gateway interface.
- Last Change: Indicates the time duration from the last time the management server was started to the time the operational state was changed to the current state for the selected gateway interface.

Gateway Channel Form

You can use the Gateway Channel form to view additional details about a discovered gateway channel.

To access the Gateway Channel form, do as follows:

1. Click **Microsoft IP Telephony**.
2. Click **Gateways**. The Gateways inventory view appears.
3. Select a gateway and click (**Open**). The Gateway form opens.
4. Click **Gateway Interface**.Select a gateway interface and click (**Open**). The Gateway Interface form opens.
5. Click **Gateway Channels**.Select a gateway channel and click (**Open**).The Gateway Channel form opens.

The Gateway Channel form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down list.

Tab	Description
Name	Indicates the name configured for the gateway channel.

The right panel displays the following tab.

- **General**: displays the general gateway channel attributes as follows.

Attribute	Description
Index	Indicates the index number configured for the gateway channel.
Type	Indicates the type of the gateway channel.
Speed	Indicates the speed of the gateway channel.
Physical Address	Indicates the physical address of the gateway channel.
Shelf	Indicates the shelf location configured for the gateway channel.
Slot	Indicates the slot configured for the gateway channel.
Port	Indicates the port number configured for the gateway channel.
Operational State	The operational state of the gateway channel. The state can display one of the following values: • Up • Down • Testing • Not Polled • Dormant • Unknown • Not Present • Lower Layer Down • No Polling Policy • Not Monitored • Not Applicable

Attribute	Description
Usage State	Indicates the usage state of the gateway channel. The state can be one of the following values: • Idle • Partially Used • Connected
Channel Number	Indicates the channel number configured for the gateway channel.
Description	Indicates the description configured for the gateway channel.
Last Change	Indicates the time duration from the last time the management server was started to the time the operational state was changed to the current state for the selected gateway channel.

- **Incidents**: Displays the incidents generated for the gateway channels discovered on the network as shown on the incidents page.

The Analysis pane displays the following details of the selected gateway channel:

- Speed: Indicates the speed of the gateway channel in number of bits in a second.
- Physical Address: Indicates the physical address of the gateway channel.
- Last Change: Indicates the time duration from the last time the management server was started to the time the operational state was changed to the current state for the selected gateway channel.

Monitoring SIP Trunk Configurations

You can use the SIP Trunks inventory view to see the SIP trunk configurations discovered on the network.

To access the SIP Trunk Configuration inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest.
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **SIP Trunk Configurations**. The SIP Trunk Configuration inventory view appears.

The SIP Trunk Configuration inventory view displays the list of SIP trunk configurations discovered on the network along with the following attributes for each SIP trunk configuration.

Attribute	Description
Identity	Indicates the unique identity of the SIP trunk configuration discovered.
Site	Indicates the Lync site that includes the SIP trunk configuration.
Description	Indicates the description configured for the SIP trunk configuration.
Management Server	Indicates if the SIP trunk configuration is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the SIP trunk discovered: • Local: If the SIP trunk configuration is being managed by the NNMi management server console on which you are viewing the server details. • Name of the regional manager that manages the SIP trunk configuration.

You can view additional details for a discovered server using the SIP Trunk Configuration form.

SIP Trunk Configuration Form

You can use the SIP Trunk Configuration form to view additional details about a discovered SIP trunk configuration.

To access the SIP Trunk Configuration form, do as follows:

1. Select a SIP trunk configuration discovered from the SIP Trunk Configuration inventory view.
2. Click (**Open**). The SIP Trunk Configuration form opens.

The SIP Trunk Configuration form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Tab	Description
Identity	Indicates the unique identity of the SIP trunk configuration discovered.

The right panel displays the **General**drop-down list that displays the general SIP trunk configuration attributes as follows.

Attribute	Description
Site	The name of the Lync site associated with the SIP trunk configuration.
Description	The description configured for the SIP trunk configuration.
RTCP Active Calls	Indicates if RTCP Active Calls is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.

Attribute	Description
RTCP Calls on Hold	Indicates if RTCP Calls on Hold is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.
SRTP Mode	Indicates if SRTP mode is required for the SIP trunk configuration.
Max Early Dialogs	Indicates the maximum early dialogs configured for the SIP trunk.
Enable Bypass	Indicates if Enable Bypass is enabled or disabled for the SIP trunk. A tick mark indicates that this feature is enabled for the SIP trunk.
Enable Signal Boost	Indicates if Enable Signal Boost is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.
Concentrated Topology	Indicates if concentrated topology is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.
Enable Mobile Trunk Support	Indicates if Enable Mobile Trunk Support is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.
Trunk Enable Refer Support	Indicates if Trunk Enable Refer Support is enabled or disabled for the SIP trunk configuration. A tick mark indicates that this feature is enabled for the SIP trunk configuration.

Monitoring Dial Plans

You can use the Dial Plans inventory view to see the dial plans discovered on the network.

To access the Dial Plans inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest.
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Dial Plans**. The Dial Plans inventory view appears.

The Dial Plans inventory view displays the list of dial plans discovered on the network along with the following attributes for each dial plan.

Attribute	Description
Identity	Indicates the unique identity of the dial plan discovered.
Name	Indicates the name configured for the dial plan.

Attribute	Description
Description	Indicates the description configured for the dial plan.
Management Server	Indicates if the dial plan is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the dial plan discovered: • Local: If the dial plan is being managed by the NNMi management server console on which you are viewing the dial plan details. • Name of the regional manager that manages the dial plan.

You can view additional details for a discovered server using the Dial Plans form.

Dial Plan Form

You can use the Dial Plans form to view additional details about a discovered dial plan.

To access the Dial Plans form, do as follows:

1. Select a dial plan discovered from the Dial Plans inventory view.
2. Click (**Open**). The Dial Plans form opens.

The Dial Plans form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down page.

Tab	Description
Identity	Indicates the unique identity of the dial plan discovered.

The right panel displays the following tabs. Click on each tab to view additional information:

- **General**: displays the general dial plan attributes as follows.

Attribute	Description
Name	Indicates the name of the dial plan.
Description	Indicates the description configured for the dial plan.
Dial in Conferencing Region	Indicates the dial in conferencing region configured for the dial plan.
Country Code	Indicates the country code configured for the dial plan.

Attribute	Description
State	Indicates the state name configured for the dial plan.
City	Indicates the city configured for the dial plan.
External Access Prefix	Indicates the external access prefix configured for the dial plan.
Optimize Device Dialing	Indicates if this attribute is enabled for the dial plan to support the configuration for an external access prefix. A tick mark next to this attribute indicates that the attribute is enabled for the dial plan.

- **Normalization Rules**: displays the normalization rules associated with the dial plan as follows

Attribute	Description
Identity	The identity of the normalization rule associated with the dial plan.
Name	The name configured for the normalization rule.
Description	The description configured for the normalization rule.

You can view more details about the normalization rules from the Normalization Rule form.

Normalization Rule Form

You can use the Normalization Rule form to view additional details about a normalization rule associated with a dial plan.

To access the Normalization Rule form, do as follows:

1. Select a normalization rule from the Normalization Rules tab on the Dial Plan form.
2. Click (**Open**). The Normalization Rule form opens.

The Normalization Rule form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down page.

Tab	Description
Identity	Indicates the unique identity of the normalization rule.

The right panel displays the **General**drop-down list that displays the general normalization rule attributes as follows.

Attribute	Description
Name	The name of the normalization rule.
Description	The description configured for the normalization rule.
Priority	Indicates the priority configured for the normalization rule.
Pattern	Indicates the pattern configured for the normalization rule.
Translation	Indicates the translation string for the normalization rule.
Is Internal Extension	Indicates if the phone number is an internal extension. A tick mark next to this attribute indicates that the phone number is an internal extension.
Do Not Use From Device	Indicates if this flag is enabled for the normalization rule. A tick mark next to this attribute indicates that the flag is enabled for the normalization rule.

Monitoring Voice Routes

You can use the Voice Routes inventory view to see the voice routes discovered on the network.

To access the Voice Routes inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest.
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Voice Routes**. The Voice Routes inventory view appears.

The Voice Routes inventory view displays the list of voice routes discovered on the network along with the following attributes for each voice route.

Attribute	Description
Identity	Indicates the unique identity of the voice route discovered.
Name	Indicates the name configured for the voice route.
Description	Indicates the description configured for the voice route.
Priority	Indicates the priority configured for the voice route.
Management Server	Indicates if the voice route is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the voice route discovered: • Local: If the voice route is being managed by the NNMi management server console on which you are viewing the voice route details. • Name of the regional manager that manages the voice route.

You can view additional details for a discovered server using the Voice Routes form.

Voice Routes Form

You can use the Voice Routes form to view additional details about a discovered voice route.

To access the Voice Routes form, do as follows:

1. Select a voice route discovered from the Voice Routes inventory view.
2. Click (**Open**). The Voice Routes form opens.

The Voice Routes form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down page.

Tab	Description
Identity	Indicates the unique identity of the voice route discovered.

The right panel displays the **General**drop-down list that displays the general voice route attributes as follows.

Attribute	Description
Name	Indicates the name of the voice route.
Description	Indicates the description configured for the voice route.
Priority	Indicates the priority configured for the voice route.
Number Pattern	Indicates the number pattern configured for the voice route.
Suppress Caller ID	Indicates if the feature to suppress the caller ID is enabled or disabled. The possible values displayed are as follows: • True • False.
Alternate Caller ID	Indicates the alternate caller ID configured if the Suppress Caller ID feature is enabled for the voice route.
PSTN Gateways	Indicates the PSTN gateway configured for the voice route.
PSTN Usages	Indicates the PSTN usage record associated with the voice route.

Monitoring Voice Policies

You can use the Voice Policies inventory view to see the voice policies discovered on the network.

To access the Voice Policies inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Voice Policies**. This displays the Voice Policies inventory view.

The Voice Policies inventory view displays the list of voice policies discovered on the network along with the following attributes for each voice policy.

Attribute	Description
Identity	Indicates the unique identity of the voice policy discovered.
Name	Indicates the name configured for the voice policy.
Description	Indicates the description configured for the voice policy.
Management Server	Indicates if the voice policy is monitored by an NNMi global manager or an NNMi regional manager This column displays one of the following values for the voice policy discovered: • Local: If the voice policy is being managed by the NNMi management server console on which you are viewing the voice policy details. • Name of the regional manager that manages the voice policy.

You can view additional details for a discovered server using the Voice Policy form.

Voice Policy Form

You can use the Voice Policy form to view additional details about a discovered voice policy.

To access the Voice Policy form, do as follows:

1. Select a voice policy discovered from the Voice Policies inventory view.
2. Click (**Open**). The Voice Policy form opens.

The Voice Policy form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down page.

Tab	Description
Identity	Indicates the unique identity of the voice policy discovered.

The right panel displays the **General**drop-down list that displays the general voice policy attributes as follows.

Attribute	Description
Name	Indicates the name of the voice policy.
Description	Indicates the description configured for the voice policy.
PSTN Usages	Indicates the PSTN usage record associated with the voice policy.
Allow Simul Ring	Indicates if the feature to allow incoming calls to ring simultaneously on additional phones is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Allow Call Forwarding	Indicates if the feature to allow call forwarding is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Allow PSTN Re Routing	Indicates if the feature to allow calls to be routed in the event of a WAN congestion or unavailability is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable Delegation	Indicates if the feature to allow calls to be delegated to other users is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable Team Call	Indicates if the feature to allow calls to be handled by a team on behalf of other members of the team is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable Call Transfer	Indicates if the feature to allow calls to be transferred is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable Call Park	Indicates if the feature to allow calls to be parked is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable Malicious Call Tracing	Indicates if the feature to allow tracing of malicious calls is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.
Enable BW Policy Override	Indicates if the feature to allow bandwidth policy override is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.

Attribute	Description
Prevent PSTN Toll Bypass	Indicates if the feature to prevent PSTN toll bypass is enabled or disabled for the voice policy. A tick mark next to this attribute indicates that this feature is enabled for the voice policy.

Monitoring Sites

You can use the Sites inventory view to see the NNMi sites discovered on the network. A site refers to an NNMi site configured by the NNMi administrator. An administrator maps the discovered Lync Server entities (edge servers, gateways, front end servers, registrar pools, and so on) on the network to the site for ease of administration.

To access the Sites inventory view, follow these steps:

1. Log on to the NNMi console as an operator or a guest.
2. Click **Microsoft IP Telephony**. This lists the following inventory options you can click to view the inventory view for that device or entity.
3. Click **Sites**. The Sites inventory view appears.

The Sites inventory view displays the list of sites discovered on the network along with the following attributes for each site:

Attribute	Description
Site Name	Indicates the name of the NNMi site.
Description	Indicates the description configured for the NNMi site.
Order	Indicates the order number configured for the NNMi site.

Launching Context-sensitive Actions for a Site

You can perform the following context-sensitive actions for a selected site from the Sites inventory view:

- Launch the call details chart detail report.
- Launch the call quality chart details report.

To launch the context-sensitive actions, do as follows:

1. Select the site.
2. Click **Actions** > **Microsoft IP Telephony**and select the appropriate option to launch the required action.

You can view additional details for a discovered server using the Sites form.

Sites Form

You can use the Sites form to view additional details about a discovered NNMi site.

To access the Sites form, do as follows:

1. Select a site discovered from the Sites inventory view.
2. Click (**Open**). The Sites form opens.

The Sites form displays information in two panels—the left panel and the right panel.

The left panel provides the following information in the **Basics** drop-down.

Tab	Description
Site Name	Indicates the name of the site discovered.

The right panel displays the **General**drop-down list that shows the general site attributes as follows.

Attribute	Description
Site Name	Indicates the name of the site.
Description	Indicates the description configured for the site.
Site Definition	Indicates the definition configured for the site.
Order	Indicates the order number configured for the site.

Viewing the Lync Enterprise Map

You can use the Lync enterprise map to view the sites, branches, gateways, server pools, servers, and gateway interfaces discovered on the network. The enterprise map displays the connection between the central site, the branch sites, the server pools. the servers, the gateways, and the gateway interfaces discovered on the network.

In addition, the map also displays the default health indicators as a label under each of the entities discovered. The NNM iSPI for IP Telephony collects these indicators from the Network Performance Server (NPS). This provides a quick reference to the status of the entity discovered and displayed on the Lync Enterprise Map. See the section Health Indicator Form to see the set of default indicators available for each entity and how you can configure the required indicators to be displayed for each entity on the map.

You can perform the following tasks using the Lync enterprise map:

- Navigate from a site to the desired level on the map as follows: *site* > *branch site* > *server pool* > *associated server* or *site* > *branch site* > *gateway* > *gateway interface*
- Save the launched maps (referred to as the child maps) to launch the map again at the same level when required.
- Specify the required default health indicators to be monitored for the entities on the map and save this configuration along with the saved map.
- Launch the call details chart detail report for a selected gateway or a Lync site or a branch.
- Launch the call quality chart details report for a selected Lync site or a branch.
- Launch the Analysis panel for a selected Lync site, branch, front end pool, server, gateway, or a gateway interface.

As an operator, the feature to launch saved maps with the set of health indicators to be monitored for the entities provides the following benefits:

- You do not have to navigate to the level of the entity that you want to monitor, every time you launch the map.
- You do not have to specify the set of indicators that you want to be monitored for each entity, every time you launch the map. The map launches with the set of indicators that you had configured for the entities. The NNM iSPI for IP Telephony retrieves the health indicators configured for the entities from the Network Performance Server (NPS), therefore, the health indicators work only if you have configured the NPS with the NNM iSPI for IP Telephony.
- The NNM iSPI for IP Telephony prompts you to launch a saved child map when you navigate to a level where you had saved a child map earlier.

Note: If you have implemented the multiple tenant model, the NNM iSPI for IP Telephony displays only the entities that the specific operator can access based on the security group-tenant combination mapped to the operator. See the section *Multiple Tenant Model for Microsoft IP Telephony* in the *NNM iSPI for IP Telephony Deployment Guide* for additional information about the multiple tenant model.

To launch the Lync enterprise map and navigate to the desired level in the map:

1. Click **Lync Enterprise Map** from the **Microsoft IP Telephony** drop-down list. This displays the Lync Enterprise Map window.
2. Right-click a Lync site and select **Enterprise Unified Communications Map** > **Drill Down**. This displays the Lync Enterprise Map with the discovered entities in the Lync site, such as the branch sites, the server pools, and the gateways.
3. Repeat *step 2* of this procedure on any of the listed entities to navigate further to the required level or the entity that you wish to see on the Lync enterprise map. For example, right-clicking

on a front end server pool and selecting **Enterprise Unified Communications Map** > **Drill Down**, displays the servers included in the front end server pool.

To launch the call details for a Lync site or branch:

1. Select a Lync site from the Lync Enterprise map
2. Click **Actions** > **IP Telephony** > **Call Detail by Lync Site**

Note: Follow the steps listed above and select the appropriate option to perform the tasks you can do from the Lync Enterprise map.

Alternatively, you can also right-click a Lync site, Lync branch, a front end server pool , a server, a gateway, or a gateway interface to launch the context-sensitive menu that lists the options to perform the tasks you can do from the Lync enterprise map.

Note: Follow the steps listed above and select the appropriate option to perform the tasks you can do from the Lync enterprise map.

Alternatively, you can also right click a Lync site, Lync branch, or a gateway to launch the context-sensitive menu that lists the options to perform the tasks you can do from the Lync enterprise map.

Related Topics:

- Save Maps
- Health Indicator Form

Saved Lync Maps

The *Saved Lync Maps* page displays a list of maps that you had saved in the past. Click **Saved Lync Maps** from the Microsoft IP Telephony drop-down list to display this page.

Note: As an operator, you can open and customize the maps and the associated health indicators for the maps that you have saved. You can also open and customize the maps and the associated health indicators saved by other operators if you belong to one of the user groups that includes the other operators.

To save a launched map, follow these steps:

1. Make sure that Single Sign-on is enabled. For information about enabling Single Sign-on, see the *HP Network Node Manager i Software* 10.00 *Deployment Reference*.
2. Click **Lync Enterprise Map** from the **Microsoft IP Telephony** drop-down list. This displays the Lync Enterprise Map window.

3. Right-click a Lync site and select **Enterprise Unified Communications MapDrill Down**. This displays the Lync Enterprise Map with the discovered entities in the Lync site, such as the branch sites, the server pools, and the gateways. Alternatively, you can also select a Lync site and click **Actions** > **Enterprise Unified Communications Map**> **Drill Down** from the menu to display the Lync Enterprise Map.

4. Repeat *step 2* of this procedure on any of the listed entities to navigate further to the required level or the entity that you wish to see on the Lync enterprise map. For example, right-clicking a front end server pool and selecting **Drill Down**, displays the servers included in the front end server pool.

5. If you wish to save the map at the level where the servers included in a server pool are displayed, you must right-click the server and select **Enterprise Unified Communications Map** > **Save Child Map**. This displays the Save Map window. Alternatively, you can also select a Lync site and click **Actions** > **Enterprise Unified Communications Map**> **Save Child Map** from the menu to display the Save Map window.

6. Type the **Map Identity** in the respective box in the Save Map window. For ease of identification, it is recommended to give meaningful values to these parameters. The *Map Identity* parameter indicates the name of the map . The Map Identity can include only alphanumeric characters. You must specify a unique name for each map that you save.

7. Click (Save) to save the map.

Note: If you open a saved map and then save the map at a new level, the NNM iSPI for IP Telephony launches the map from the new level the next time you launch the saved map.

Launching Saved Maps

To launch saved maps, do as follows:

1. Click **Saved Lync Maps** from the **Microsoft IP Telephony** drop-down list. This opens the Open Saved Map window.

2. Select the **Map Identity** required from the drop-down list.

3. Click **Open** to launch the saved map.

Note: Alternatively, you can launch a saved map when you navigate to a level where you had saved a child map earlier. The NNM iSPI for IP Telephony prompts you launch an existing child map or the default map.

Deleting Saved Maps

To delete saved maps, do as follows:

1. Click **Saved Lync Maps** from the **Microsoft IP Telephony** drop-down list. This opens the Open Saved Map window.
2. Select the **Map Identity** required from the drop-down list.
3. Click **Delete** to delete the map selected.

Note:

- You can only delete the maps that you have saved and the maps created by the operators who belong to one of the user groups that include you.
- You can select a **Map Identity** and click **Delete** to remove the *Map Identity*.

Health Indicator Form

The Health Indicator Form helps you to specify the health indicators to be monitored for the following entities on the enterprise map:

- Microsoft Lync central site
- Microsoft Lync branch site
- Servers associated with the central site or the branch site
- Gateways
- Gateway interfaces

The NNM iSPI for IP Telephony collects the values for the indicators from the Network Performance Server and displays the values as a label below the respective entity on the Lync Enterprise Map. After specifying the health indicators to be monitored for the required entity, the next time you launch the map that includes the specific entity, the NNM iSPI for IP Telephony launches the map with the health indicators you had specified.

To access the Health Indicator Form:

> **Note:** You cannot configure health indicators if NPS and SiteScope are not installed in the environment or configured to work with the NNM iSPI for IP Telephony.

1. Click **Lync Enterprise Map** from the **Microsoft IP Telephony** drop-down list. This displays the Lync Enterprise Map window.
2. Right-click a Lync site and select **Enterprise Unified Communications Map** > **Health Indicators**. This displays the Health Indicators window for the Lync site on the Site Health Indicators tab page. Alternatively, you can also select a Lync site and click **Actions** > **Enterprise Unified Communications Map**> **Health Indicators** from the menu to display the

Health Indicators window.

Note: You can navigate to any of the listed entities for which NNM iSPI for IP Telephony allows you to specify the health indicators and perform this step to launch the Health Indicators window for the specific entity.

3. Select the map identity for which you want to configure the health indicators from the **Map Identity** drop-down list. If you do not select a map identity, the NNM iSPI for IP Telephony uses the default health indicators when launching the default Lync enterprise map.
4. Select the required health indicators from the **Select the Health Indicators** section.
5. Select an interval of your choice from the **Interval** drop-down list for each indicator. The NNM iSPI for IP Telephony uses this interval to collect the health indicators from the NPS.
6. You can select the **Apply these settings to all entities of this type for the selected map name** option to select all the similar health indicators on the selected map name and apply the specified interval for all these entities.
7. Click (the **Save** icon) to save the selected health indicators for the entity.

The Health Indicators window displays the health indicators specific to each entity depending on the entity you selected. For the servers in a front end pool, this window provides options to select the indicators based on the role the server plays. You can select from the following list of options:

- Front end server
- Audio video conferencing server
- Registrar server
- Mediation server

Filtering Central Sites

The Central Sites Filter page allows you to select the list of central sites that you want the NNM iSPI for IP Telephony to display on the Lync Enterprise map. After specifying the list of central sites that you want to see, you can associate this list with a map name that you had saved earlier. The next time you launch the map, the map displays only the central sites that you had selected.

To filter the list of central sites, follow these steps:

1. From the **Microsoft IP Telephony** drop-down list, click **Lync Enterprise Map**. This displays the Lync Enterprise Map window.
2. Click **Actions** > **Enterprise Unified Communications Map** > **Map Filter**. This displays the Central Sites Filter Window.

3. From the List of Central Sites drop-down list, select the central sites that you want to be included in the Enterprise Map and click . The NNM iSPI for IP Telephony moves the selected central sites to the **Selected Central Sites** list box. You can select multiple central sites by pressing the **Ctrl** (Control) key.

4. Select the map name to which you want to associate this selection from the **Map Name** drop-down list.

5. Click (the **Save** icon) to save the changes.

Nortel IP Telephony

The Nortel IP Telephony workspace enables you to view the inventory views for the Nortel devices and entities that are discovered and monitored in your environment. The following table lists the options that you can click to view the details of a discovered device or an entity:

Inventory View	Purpose
Call Servers	Lists the Nortel Call Servers discovered on the network.
Signaling Servers	Lists the Nortel Signaling Servers discovered on the network.
IP Phones	Lists the Nortel IP Phones discovered on the network.
Media Gateways	Lists the Nortel Media Gateways discovered on the network.

Monitoring Nortel Call Servers

The Call Servers view displays a list of available Nortel Call Servers in the network. The view arranges the key attributes of all discovered Nortel Call Servers in a table.

To launch the Call Servers view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > Call Servers**. The Call Servers view opens in the right pane.

Basic Attributes of the Nortel Call Servers Table

Attribute	Description
Node Status	The status of the Nortel Call Server. Possible values are: • No Status • Normal • Disabled • Warning • Minor • Major • Critical • Unknown
Name	The system name of the Nortel Call Server.
IP Address	The IP address of the Nortel Call Server.
Model	The model of the Nortel Call Server.
Version	Version of the Nortel Call Server.
Description	A description of the Nortel Call Server.
Management Server	The management server for the call server. This attribute displays one of the following values: • **Local**: If the call server is being managed by the NNMi management server console on which you are viewing the call server details. • Name of the regional manager that manages the call server.

View the Nortel Call Server Details Form

You can view the details of a single Nortel Call Server in a form, which you can launch from the Nortel Call Servers view.

To view the Nortel Call Server Details Form:

In the Nortel Call Servers view, select the node of your interest, and then click . The Nortel Call Server Details Form opens. The Nortel Call Server form displays details of the selected server in the left pane, and details of all the associated Nortel Signaling Servers in the right pane.

To view the Node Form for the Nortel Call Server, click , and then click **Open**. The Node Form opens displaying the details of the server.

Analysis Pane

The Analysis pane displays a summary of the details of the selected call controller as follows:

Nortel Call Server Details Summary tab

- Name: The name of the selected call server.

Call Server Information tab

- Management Mode: The management state of the call server. The status can be one of the following strings: Managed, Unmanaged, or Out of Service.
- IP Address: The IP address of the call server.
- ELAN IP Address: The IP address of the interface that is connected to the ELAN where the call server belongs.
- Model: The model of the call server.
- Description: The description of the call server.

Device Registrations tab

- Number of Associated Signaling Servers: The number of signaling servers associated with the call server.

Filtering Nortel Call Servers

You can filter the listed call servers in the Call Servers view based on the management server.

To filter the Port Networks view, follow these steps:

1. Right-click the **Management Server** attribute column of one of the call servers listed in the Call Servers view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the call servers that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the call servers for which the selected column is not empty.
   - **Is empty**: filters and lists all the call servers for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the call servers that do not have the value in the column that you selected.

     The filtered list of call servers appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Nortel Call Server form

The Nortel Call Server Details Form helps you view the node details of the selected Nortel Call Server and the Signaling Servers and IP phones associated with it. The form presents two different panes.

The right pane lists the following details:

- Associated Signaling Servers: The Associated Signaling Servers tab displays the details of all the Signaling Servers associated with the selected server. The tab displays the details of every associated Signaling Servers in the format presented in the Nortel Signal Servers view.
- Associated IP phones: The Associated Extensions tab displays the details of all the IP phones associated with the selected Nortel Call Server. The tab displays the details of every associated IP phone in the format presented in the Nortel IP Phones view.
- Incidents: This tab displays the incidents related to the changes in the state of the Call Server.

The left pane lists the following details of the selected Nortel Call Server:

Basic Attributes of the Selected Nortel Call Server

Attribute	Description
Hosted Node	The hostname of the Nortel Call Server node.
Name	The name of the Nortel Call Server.
IP Address	The IP address of the Nortel Call Server.
Description	A short description of the server.
Version	The version of the server.
ELAN IP	IP address of the interface that is connected to the ELAN where the Nortel Call Server belongs.
Model	Model of the Nortel Call Server.

Monitor Nortel Signaling Servers

The Signaling Servers view displays a list of available Nortel Signaling Servers in the network. The view arranges the key attributes of all discovered Nortel Signaling Servers in a table.

To launch the Nortel Signaling Servers view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > Signaling Servers**. The Signaling Servers view opens in the right pane.

Basic Attributes of the Nortel Signaling Servers Table

Attribute	Description
Node Status	The status of the Nortel Signaling Server. Possible values are: • No Status • Normal • Disabled • Warning • Minor • Major • Critical • Unknown
Name	The fully-qualified domain name of the Nortel Signaling Server.
IP Address	The IP address of the Nortel Signaling Server.
Description	Description of the Nortel Signaling Server.
Model	The model of the Nortel Signaling Server.
Version	Version of the Nortel Signaling Server.
Call Servers	The associated Nortel Call Servers.
Management Server	The management server for the signaling server. This attribute displays one of the following values: • **Local**: If the signaling server is being managed by the NNMi management server console on which you are viewing the signaling server details. • Name of the regional manager that manages the signaling server.

View the Nortel Signaling Server Details Form

You can view the details of a single Nortel Signaling Server in a form, which you can launch from the Nortel Signaling Servers view.

To view the Nortel Signaling Server Details Form:

In the Nortel Signaling Servers view, select the node of your interest, and then click . The Nortel Signaling Server Details Form opens. The Nortel Signaling Server Details Form displays details of

the selected signaling server in the left pane, and details of all the associated Nortel Call Servers in the right pane.

To view the Node Form for the Nortel Signaling Server, click , and then click **Open**. The Node Form opens displaying the details of the server.

Analysis Pane

The Analysis pane displays a summary of the details of the selected call controller as follows:

Nortel Signaling Server Details Summary tab

- Name: The name of the selected signaling server.

Call Server Information tab

- Management Mode: The management state of the signaling server. The status can be one of the following strings: Managed, Unmanaged, or Out of Service.
- IP Address: The IP address of the signaling server.
- ELAN IP Address: The IP address of the interface that is connected to the ELAN where the signaling server belongs.
- TLAN IP Address: The IP address of the interface that is connected to the TLAN where the signaling server belongs.
- Model: The model of the signaling server.
- Description: The description of the signaling server.

Device Registrations tab

- Number of Associated Call Servers: The number of call servers associated with the signaling server.

Filtering Nortel Signaling Servers

You can filter the listed signaling servers in the Signaling Servers view based on the management server.

To filter the Signaling Servers view, follow these steps:

1. Right-click the **Management Server** attribute column of one of the signaling servers listed in the Signaling Servers view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the signaling servers that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.

- **Is not empty**: filters and lists all the signaling servers for which the selected column is not empty.
- **Is empty**: filters and lists all the signaling servers for which the selected column is empty.
- **Not equal to this value**: filters and lists all the signaling servers that do not have the value in the column that you selected.

  The filtered list of signaling servers appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Nortel Signaling Server Details Form

The Nortel Signaling Server form helps you view the node details of the selected Nortel Signaling Server and the Nortel Call Servers and QOS Zones associated with it. The form presents two different panes.

The right pane lists the following details:

- Associated CallServers: The Associated CallServers tab displays the details of all the Nortel Call Servers associated with the selected server. The tab displays the details of every associated Nortel Call Servers in the format presented in the Nortel Call Servers view.
- Associated QOS Zones: The Associated QOS Zones tab displays the details of all the QoS zones configured with the selected Nortel Signal Server. The tab displays the details of every associated QoS zone in the format presented in the Nortel QOS Zone Table view.
- IP Phones: This tab displays the IP phones associated with the Signaling Server as shown on the IP Phones page.

The left pane lists the following details of the selected Nortel Signaling Server:

Basic Attributes of the Selected Nortel Signaling Server

Attribute	Description
Hosted Node	The hostname of the Nortel Signaling Server node.
Name	The name of the Nortel Signaling Server.
IP Address	The IP address of the Nortel Signaling Server detected by NNMi.
Version	The version of the server.
Description	A short description of the server.
Model	Model of the Nortel Signaling Server.

Basic Attributes of the Selected Nortel Signaling Server, continued

Attribute	Description
ELAN IP Address	IP address of the interface that is connected to the ELAN where the Nortel Signaling Server belongs.
Host IP Addresses	All the IP addresses of the Nortel Signaling Server.
TLAN IP Address	IP address of the interface that is connected to the TLAN where the Nortel Signaling Server belongs.
TPS Service	Indicates if the TPS service is enabled on the signaling server.

Nortel QOS Zones Table View

The QOS Zones table view displays the QoS metrics of all the configured QoS zones on a Nortel Signaling Server. The view arranges the QoS metrics in a table.

Basic Attributes of the Nortel QOS Zones Table

Attribute	Description
QOS Zone ID	The ID of a QoS zone.
Name	The name of the QoS zone. The name is formed using the IP address of the Nortel Signaling Server and the QoS Zone number.
Signaling Server IP Address	The IP address of the Signaling Server on which the QOS zone was configured.
Management Server	The management server for the QoS zone. This attribute displays one of the following values: • **Local**: If the QoS zone is being managed by the NNMi management server console on which you are viewing the QoS zone details. • Name of the regional manager that manages the QoS zone.

View the Nortel QOS Zone Details form

You can view the details of QOS zones in a form, which you can launch from the Nortel QOS Zones Table view.

To view the Nortel QOS Zone Details form:

In the Nortel QOS Zones table view, select the node of your interest, and then click . The Nortel QOS Zone Details Form opens. The Nortel QOS Zone Details Form displays details of the QoS zone in the left pane, and details of set parameters in the right pane.

Filtering Nortel QOS Zones

You can filter the listed QOS zones in the QOS Zones view based on the management server.

To filter the QOS Zones view, follow these steps:

1. Right-click the **Management Server** attribute column of one of the QOS zones listed in the QOS Zones view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the QOS zones that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the QOS zones for which the selected column is not empty.
   - **Is empty**: filters and lists all the QOS zones for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the QOS zones that do not have the value in the column that you selected.

     The filtered list of QOS zones appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

View the Nortel QOS Zone Details Form

The Nortel QOS Zone Details Form includes the details of a particular QoS zone that was configured on a Nortel Signaling Server.

The left pane lists the following details:

- QOS Zone ID
- Name of the QoS zone
- IP address of the Signaling Server where the QoS zone was configured.

The right pane introduces two tabs—**Intra Zone QOS Parameters** and **Inter Zone QOS Parameters**.

The Intra Zone QOS parameter tab presents you the following metrics:

Basic Attributes of the Intra Zone QOS Parameters tab

Attribute	Description
CallsMadeIn	The number of calls made successfully within the selected zone.
CallsBlockedIn	The number of calls blocked within the selected zone.
PeakIn	The percentage peak bandwidth within the selected zone.
AvgIn	The percentage average bandwidth within the selected zone.
InThrViol	Violation of bandwidth-usage threshold within the selected zone.
IntervalIn	The number of measuring-interval samples within the selected zone.
UnacpLatencyIn	The number of unacceptable latency samples within the selected zone.
UnacpPacketLossIn	The number of unacceptable packet loss within the selected zone.
UnacpJitterIn	The number of unacceptable jitter samples within the selected zone.
UnacpRFactorIn	The number of unacceptable R-factor samples within the selected zone.
UnacpEchoRLossIn	The number of unacceptable Echo Return Loss within the selected zone.
WarnLatencyIn	The number of warning latency samples within the selected zone.
WarnJitterIn	The number of warning jitter samples within the selected zone.
WarnPacketLossIn	The number of warning packet-loss samples within the selected zone.
WarnRFactorIn	The number of warning R-factor samples within the selected zone.
WarnEchoRLossIn	The number of warning Echo Return Loss within the selected zone.

The Inter Zone QOS parameter tab presents you the following metrics:

Basic Attributes of the Inter Zone QOS Parameters tab

Attribute	Description
CallsMadeOut	The number of calls made successfully within different zones.
CallsBlockedOut	The number of calls blocked within different zones.
PeakOut	The percentage peak bandwidth within different zones.
AvgOut	The percentage average bandwidth within different zones.
OutThrViol	Violation of bandwidth-usage threshold within different zones.
IntervalOut	The number of measuring-interval samples within different zones.
UnacpLatencyOut	The number of unacceptable latency samples within different zones.
UnacpPacketLossOut	The number of unacceptable packet loss within different zones.

Basic Attributes of the Inter Zone QOS Parameters tab, continued

Attribute	Description
UnacpJitterOut	The number of unacceptable jitter samples within different zones.
UnacpRFactorOut	The number of unacceptable R-factor samples within different zones.
UnacpEchoRLossOut	The number of unacceptable Echo Return Loss within different zones.
WarnLatencyOut	The number of warning latency samples within different zones.
WarnJitterOut	The number of warning jitter samples within different zones.
WarnPacketLossOut	The number of warning packet-loss samples within different zones.
WarnRFactorOut	The number of warning R-factor samples within different zones.
WarnEchoRLossOut	The number of warning Echo Return Loss within different zones.

The Incidents tab lists the incidents generated for state changes for the Nortel QoS Zones.

In this form, you can view the following details:

- Value of a QoS metric
- The threshold set for the metric
- If the metric value has violated the set threshold

If you want to set the thresholds for these metrics, you must log on to the NNMi console with an administrative or operator level 2 privileges.

For more information to set thresholds for Nortel QoS zone metrics, see Set thresholds for Nortel QoS metrics.

Nortel IP Phones View

The IP Phones view displays a list of available Nortel IP phones on the network. The view arranges the key attributes of all discovered Nortel IP phones in a table.

To launch the IP Phones view, follow this step:

- From the **Workspaces** navigation pane, click **Nortel IP Telephony > IP Phones**. The IP Phones view opens in the right pane.

Basic Attributes of the IP Phones Table

Attribute	Description
Registration State	The registration state of the IP phone. The registration state can be Registered or Unregistered.

Basic Attributes of the IP Phones Table, continued

Attribute	Description
Extension Number	The extension number of the IP phone.
Model	The model of the IP phone.
IP Address	The IP address of the phone.
Call Server	The fully-qualified domain name or IP address of the Nortel Call Server to which the IP phone belongs.
Description	A description of the IP phone.
Management Server	The management server for the IP phone. This attribute displays one of the following values: ▪ **Local**: If the IP phone is being managed by the NNMi management server console on which you are viewing the IP phone details. ▪ Name of the regional manager that manages the IP phone.

View the Nortel Phone Detailed form

You can view the details of a single Nortel IP phone in a form, which you can launch from the Nortel IP Phone Details Form.

To view the Nortel IP Phone Details form, follow thos step:

- In the IP Phones view, select the node of your interest, and then click . The Nortel Phone Detailed form opens. The Nortel IP Phone Details Form displays details of the selected phone in the left pane, and details of the associated Nortel Call Server in the right pane.

To view the Node Form for the Nortel IP phone, click , and then click **Open**. The Node Form opens displaying the details of the phone.

Filtering Nortel IP phones

You can filter the listed IP phones in the IP Phones view with the available filters. You can perform the filtering action only on the **Registration State**, **Extension Number**, and **Management Server** columns.

Note: You can select multiple filters based on your requirements.

To filter the IP Phones view, follow these steps:

1. Right-click the **Registration State**, **Extension Number**, or **Management Server** attribute of one of the IP phones listed in the IP Phones view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the IP phones that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the IP Phones for which the selected column is not empty.
   - **Is empty**: filters and lists all the IP Phones for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the IP phones that do not have the value in the column that you selected.

The filtered list of Nortel IP phones appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

Nortel Phone Detailed form

The Nortel IP Phone Details Form helps you view the node details of the selected IP phone and the Nortel Call servers associated with it. The form presents two different panes.

The right pane lists the following details:

- Associated CallServers: The Associated CallServers tab displays the details of the Nortel Call server associated with the selected IP phone. The tab displays the details of the associated Nortel Call Server in the format presented in the Nortel Call Server view.
- Signaling Server: The signaling server details associated with the IP phone as shown on the Signaling Server page.
- Incidents: This tab lists the incidents related to the Nortel IP Phone.

The left pane lists the following details of the selected Nortel IP phone:

Basic Attributes of the Selected Nortel IP Phone

Attribute	Description
Registration State	The registration state of the IP phone line.
IP Address	The IP address of the phone.

Basic Attributes of the Selected Nortel IP Phone, continued

Attribute	Description
Extension Number	Extension number of the phone.
Description	A short description of the phone.
Model	The model of the phone.
Vendor	The name of the vendor, in this case, Nortel.
Controller	The IP address of the Nortel Call Server that controls the phone.
SS TLAN IP Address	The TLAN IP address of the signaling server associated with the IP phone.

Monitoring Nortel Media Gateways

The Media Gateways view displays a list of available Nortel media gateway devices on the network. The view arranges the key attributes of all discovered Nortel media gateway devices in a table.

To launch the Nortel Media Gateways view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > Media Gateways**. The Nortel Media Gateways view opens in the right pane.

Basic Attributes of the Nortel Media Gateways Table

Attribute	Description
IP Address	The IP address of the Nortel media gateway device.
Type	The type of the Nortel media gateway device. Possible types are: Voice Gateway Media Card (**VGMC**) and Media Gateway Controller (**MGC**).
Call Server	The fully-qualified domain name of the CS1000 server to which the gateway device is configured.
Protocol	The protocol used by the gateway device.
Description	A description of the media gateway device.
Management Server	The management server for the media gateway device. This attribute displays one of the following values: • **Local**: If the media gateway device is being managed by the NNMi management server console on which you are viewing the media gateway device details. • Name of the regional manager that manages the media gateway device.

View the Nortel Media Gateway form

You can view the details of a single Nortel media gateway in a form, which you can launch from the Nortel Media Gateways view.

To view the Nortel Media Gateway form:

In the Nortel Media Gateways view, select the node of your interest, and then click . The Nortel Media Gateway Details Form opens. The Nortel Media Gateway Details Form displays details of the selected gateway in the left pane, and details of all the associated Nortel Call Servers in the right pane.

To view the Node Form for the media gateway, click , and then click **Open**. The Node Form opens displaying the details of the gateway.

Filtering Nortel Media Gateways

You can filter the listed media gateways in the Media Gateways view based on the management server.

To filter the Media Gateways view:

1. Right-click the **Management Server** attribute column of one of the media gateways listed in the Media Gateways view.
2. Select one of the following filters:
   - **Equals this value**: filters and lists all the media gateways that have a value that is equal to the value of the column that you selected.
   - **Create Filter**: opens the Filter dialog box. This dialog box helps you specify a string and select options to perform filtering based on the string specified.
   - **Is not empty**: filters and lists all the media gateways for which the selected column is not empty.
   - **Is empty**: filters and lists all the media gateways for which the selected column is empty.
   - **Not equal to this value**: filters and lists all the media gateways that do not have the value in the column that you selected.

     The filtered list of media gateways appears in the view.

Note: After viewing the filtered list, always remove the filter. To remove the filter, right-click the filter attribute, and then click **Remove Filter**.

View the Nortel Media Gateway Details Form

The Nortel Media Gateway Details Form helps you view the node details of the selected Nortel media gateway and the Nortel Call servers associated with it. The form presents two different panes.

The right pane lists the following details:

- Associated CallServers: The Associated CallServers tab displays the details of all the Nortel Call servers associated with the selected media gateway. The tab displays the details of every associated Call Server in the format presented in the Nortel Call Server view.

The left pane lists the following details of the selected Nortel media gateway:

Basic Attributes of the Selected Nortel Media Gateway

Attribute	Description
Hosted Node	Hostname of the media gateway.
Name	The name of the media gateway.
Model	The model of the media gateway.
Description	A short description of the media gateway.
Vendor	Nortel
ELAN IP	IP address of the interface that is connected to the ELAN where the gateway belongs.
TLAN IP	IP address of the interface that is connected to the TLAN where the gateway belongs.

Incidents Collected from the ClarusIPC Environment

If you integrate the ClarusIPC deployment with the NNM iSPI for IP Telephony, you can view different incidents that originate from the ClarusIPC environment.

Incidents Collected from the ClarusIPC Environment

Incident	Message	Severity	Description
clarusipcPolicyChangeNotification	A Configuration Change alert has occurred for Policy "$1:$5" on Cluster "$3:$2"] Reason="$4"	Warning	A ClarusIPC Change alert was generated as a result of a policy violation.
clarusipcPolicyTestTrap	$1	Normal	This is a test SNMP policy trap.
clarusipcTaskInitiation	Task "$1" initiated	Normal	An informational notification indicating the start of a ClarusIPC task. All other task-related notifications follow this incident.

Incidents Collected from the ClarusIPC Environment, continued

Incident	Message	Severity	Description
clarusipcTPErr	[TestPlan "$5" against Cluster "$3" Contains Errors] Passed=$7; Failed=$9; Errors=$8; Task="$1"; Duration=$10; Message="$4"	Major	A ClarusIPC test plan executed with errors.
clarusipcTPFail	[TestPlan "$5" against Cluster "$3" Contains Failures] Passed=$7; Failed=$9; Errors=$8; Task="$1"; Duration=$10; Message="$4"	Critical	A ClarusIPC test plan executed with failures but no errors.
clarusipcTPPass	[TestPlan "$5" against Cluster "$3" Passed] Passed=$7; Failed=$9; Errors=$8; Task="$1"; Duration=$10; Message="$4"	Normal	A ClarusIPC test plan executed with no failures or errors.
clarusipcTaskSyncFailed	[Sync Failed for Task "$1" on Cluster "$3"] next Attempt=$2; Message="$4"	Major	A synchronization with the specified cluster failed.

If you disable the ClarusIPC integration, you must manually remove the ClarusIPC-specific incidents from the SNMP Trap Configuration (by Name) tab in the Incident Configuration window.

Context-Sensitive URLs for ClarusIPC Incidents

If you integrate the ClarusIPC deployment with the NNM iSPI for IP Telephony, three context-sensitive URL action items appear in the views for incident browsing.

Context-Sensitive URLs for ClarusIPC Incidents

URL Name	Description
IPT Edit Policy	Helps you view the list of ClarusIPC alert rules for the selected incident
IPT Detailed Info	Helps you view the details of the selected incident
IPT Test Results	Helps you access the ClarusIPC test results of the selected incident

To use these URLs, select the incident from the view for incident browsing, and then click **Actions**.

Incidents Generated by the NNM iSPI for IP Telephony

When specific events occur in the IP telephony environment, the NNM iSPI for IP Telephony sends incidents with appropriate messages to the NNMi incident view. This section describes the incidentsthat are genarated by the NNM iSPI for IP Telephony for the Cisco, Avaya, Nortel, Microsoft and Acme IP telephony environments.

Acme IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony

Acme IP Telephony Incident	Message	Severity	Description
AcmeSBCSDRedundancyStateStandby	Session Director with IP address: $ipAddress is in Standby state	Warning	The Session Director is in Standby state.
AcmeSBCSDRedundancyStateOutOfService	Session Director with IP address: $ipAddress is in Out of Service state	Warning	The Session Director is in Out of Service state.
AcmeSBCSDRedundancyStateInitial	Session Director with IP address: $ipAddress is in Initial state	Warning	The Session Director is in Initial state.
AcmeSBCSDRedundancyStateActive	Session Director with IP address: $ipAddress is in Active state	Normal	The Session Director is in Active state.
AcmeSBCSessionAgentDisabled	Disabled Session Agent $hostname on Session Director $ipAddress	Warning	The Session Agent is in Disable state.
AcmeSBCSessionAgentOutOfService	OutofService Session Agent $hostname on Session Director $ipAddress	Warning	The Session Agent is in Out of Service state.
AcmeSBCSessionAgentStandby	Standby Session Agent $hostname on Session Director $ipAddress	Warning	The Session Agent is in Standby State.

Acme IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Acme IP Telephony Incident	Message	Severity	Description
AcmeSBCRealmCallLoadReduction	Call Load Reduction on Realm $realmName on Session Director with IP address: $ipAddress	Warning	The Realm is in Call Load ReductionState.
AcmeSBCRealmConstraintViolation	Constraint Violation on Realm $realmName on Session Director with IP address: $ipAddress	Warning	The Realm is in Constraint Violated State
AcmeSBCRealmInService	InService on Realm $realmName on Session Director with IP address: $ipAddress	Normal	The Realm is in InService State
AcmeSBCSessionAgentInService	InService Session Agent $hostname on Session Director $ipAddress	Normal	The Session Agent is in In Service State
AcmeSBCSessionAgentConstraintsViolation	Constraint Violation Session Agent $hostname on Session Director $ipAddress	Warning	The Session Agent is in Constraint Violated State
AcmeSBCSessionAgentInServiceTimedOut	Service Timed Out Session Agent $hostname on Session Director $ipAddress	Warning	The Session Agent is in Service Timed out state
AcmeSBCSessionAgentOosprovisionedresponse	OosProvisionedResponse Session Agent $hostname on Session Director $ipAddress	Warning	The Session Agent is in OosProvisionedResponse State

Acme IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Acme IP Telephony Incident	Message	Severity	Description
AcmeSBCCallTerminationReason	Call terminated reason matches the Monitored Call Termination Reason for call from $CallingPartyNumber to $CalledPartyNumber	Warning	This incident is generated when the Acme Session Director call termination cause code matches with the configured value

Acme IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Acme IP Telephony Incident	Message	Severity	Description
AcmeSBCLowQOSCall	Low QOS/MOS: CallingJitter: $CallingQOSJitter ms, Calling Latency: $CallingQOSLatency ms, Calling Average MOS: $CallingQOSMOS, % of Calling Packets Lost: $CallingQOSPacketLoss, CallingQOSRFactor: $CallingQOSRFactor, CalledJitter: $CalledQOSJitter ms, Called Latency: $CalledQOSLatency ms, Called Average MOS: $CalledQOSMOS, % of Called Packets Lost: $CalledQOSPacketLoss, CalledQOSRFactor: $CalledQOSRFactor, during a call from $CallingPartyNumber to $CalledPartyNumber breached set threshold (Jitter: $jitterThreshold ms, Latency: $latencyThreshold ms, Average MOS: $MOSThreshold, PPL: $PPLThreshold, RFactor: $RFactorThreshold)	Warning	

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony

Avaya IP Telephony Incident	Message	Severity	Description
AvayaECCStatusActive	Physical Avaya CM Server with IP address: $ipAddress in CM Primary Server pair $serverPairIPAddr is in Active state.	Normal	The paired Avaya Primary Server is in the active state.
AvayaECCStatusBusyout	Physical Avaya CM Server with IP address: $ipAddress in CM Primary Server pair $serverPairIPAddr is in busyout state.	Warning	The paired Avaya Primary Server is in the busyout state.
AvayaECCStatusDormant	Physical Avaya CM Server with IP address: $ipAddress in CM Primary Server pair $serverPairIPAddr is in dormant state.	Warning	The paired Avaya Primary Server is in the dormant state.
AvayaECCStatusStandby	Physical Avaya CM Server with IP address: $ipAddress in CM Primary Server pair $serverPairIPAddr is in standby state.	Warning	The paired Avaya Primary Server is in the standby state.
AvayaIncIncomingPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Incoming Trunk Load metric Incoming Peg = $loadincIncIncomingPeg for measurement hour $loadincMeasHour.	Warning	This incident is generated when the Incoming Trunk Load, Incoming Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaIncIncomingUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Incoming Trunk Load metric Incoming Use = $loadincIncIncomingUse for measurement hour $loadincMeasHour.	Warning	This incident is generated when the Incoming Trunk Load, Incoming Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaIncIntraPNPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Incoming Trunk Load metric Intra PN Peg = $loadincIncIntraPNPeg for measurement hour $loadincMeasHour.	Warning	This incident is generated when the Incoming Trunk Load, Intra PN Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaIncIntraPNUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Incoming Trunk Load metric Intra PN Peg = $loadincIncIntraPNPeg for measurement hour $loadincMeasHour.	Warning	This incident is generated when the Incoming Trunk Load, Intra PN Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaIncOutgoingPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Incoming Trunk Load metric Outgoing Peg = $loadincIncOutgoingPeg for measurement hour $loadincMeasHour.	Warning	This incident is generated when the Incoming Trunk Load, Outgoing Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network.
AvayaIncOutgoingUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Incoming Trunk Load metric Outgoing Use = $loadincIncOutgoingUse for measurement hour $loadincMeasHour.	Warning	This incident is generated when the Incoming Trunk Load, Outgoing Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaIntInterPNPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Intercom metric Inter PN Peg = $loadintIntInterPNPeg for measurement hour $loadintMeasHour.	Warning	This incident is generated when the Intercom Inter PN Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaIntInterPNUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Intercom metric Inter PN Use = $loadintIntInterPNUse for measurement hour $loadintMeasHour.	Warning	This incident is generated when the Intercom Inter PN Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaIntIntraPNPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Intercom metric Intra PN Peg = $loadintIntIntraPNPeg for measurement hour $loadintMeasHour.	Warning	This incident is generated when the Intercom Intra PN Peg Parameter in the Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaIntIntraPNUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Intercom metric Intra PN Use = $loadintIntIntraPNUse for measurement hour $loadintMeasHour.	Warning	This incident is generated when the Intercom Intra PN Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaMGwModuleStatusFaultActive	Fault Active: Avaya Media Module with Id $slotNumber in H248 Media Gateway: $gatewayIpAddress with Media Gateway number $h248MgwNumInCM in Primary CM $cmIpAddress.	Warning	This incident is generated when the Avaya Media Gateway Media module is in the Fault Active status.
AvayaMGwStatusUnregistered	Unregistered: Avaya H248 Media Gateway: $gwIpAddress with Media Gateway number $h248MgwNumInCM in Primary CM $cmIpAddress.	Critical	This incident is generated when the Avaya Media Gateway is in the Unregistered state
AvayaMGwVoIPEngineStatusFaultActive	Fault Active on Avaya VoIP Engine Id $slotNumber of Avaya Media Gateway $gatewayIpAddress.	Warning	This incident is generated when the VoIP Engine is in the Fault Active status.
avayaNetRegionConnBWUsedRxViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region connection from $source to $destination Receive bandwidth used = $bwUsedRx	Warning	This incident is generated when the Receive bandwidth used breaches the threshold you specified for an Avaya IP Network Region Connection

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
avayaNetRegionConnBWUsedTxViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region connection from $source to $destination Transmit bandwidth used = $bwUsedTx	Warning	This incident is generated when the Transmit bandwidth used breaches the threshold you specified for an Avaya IP Network Region Connection
avayaNetRegionConnNbrConnRxViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region connection from $source to $destination Receive Connection count = $connCountRx	Warning	This incident is generated when the Receive Connection count breaches the threshold you specified for an Avaya IP Network Region Connection
avayaNetRegionConnNbrConnTxViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region connection from $source to $destination Transmit Connection count = $connCountTx	Warning	This incident is generated when the Transmit Connection count breaches the threshold you specified for an Avaya IP Network Region Connection

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaOutIncomingPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Outgoing Trunk Load metric Incoming Peg = $loadoutOutIncomingPeg for measurement hour $loadoutMeasHour.	Warning	This incident is generated when the Outgoing Trunk Load, Incoming Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaOutIncomingUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Outgoing Trunk Load metric Incoming Use = $loadoutOutIncomingUse for measurement hour $loadoutMeasHour.	Warning	This incident is generated when the Outgoing Trunk Load, Incoming Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaOutIntraPNPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Outgoing Trunk Load metric Intra PN Peg = $loadoutOutIntraPNPeg for measurement hour $loadoutMeasHour.	Warning	This incident is generated when the Outgoing Trunk Load, Intra PN Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaOutIntraPNUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Outgoing Trunk Load metric Intra PN Use = $loadoutOutIntraPNUse for measurement hour $loadoutMeasHour.	Warning	This incident is generated when the Outgoing Trunk Load, Intra PN Use Parameter in Avaya Port Network, has breached the threshold you specified an Avaya Port Network
AvayaOutOutgoingPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Outgoing Trunk Load metric Outgoing Peg = $loadoutOutOutgoingPeg for measurement hour $loadoutMeasHour.	Warning	This incident is generated when the Outgoing Trunk Load, Outgoing Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaOutOutgoingUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Outgoing Trunk Load metric Outgoing Use = $loadoutOutOutgoingUse for measurement hour $loadoutMeasHour.	Warning	This incident is generated when the Outgoing Trunk Load, Outgoing Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaPNOccViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber metric PN Link Occupancy = $loadtotalPNOccupancy for measurement hour $loadtotalMeasHour.	Warning	This incident is generated when the PN Link Occupancy Parameter in Avaya Port Network PN Link Occupancy Resource, has breached the threshold you specified for an Avaya Port Network
AvayaPhoneUnknown	Avaya IP Phone registration state Unknown: Primary CM $controllerIPAddress.	Warning	The Avaya Phone has changed its state to Unknown
AvayaPhoneUnregistered	Avaya IP Phone unregistered: Primary CM $controllerIPAddress.	Warning	The Avaya Phone is unregistered
AvayaRPQueOvflowThreVio	Threshold Breached:Avaya Primary CM $hostNodeIP Route Pattern $rpNumber Queue Overflow counts = $queueOvflow for measurement hour $rpMeasHour.	Warning	Queue Overflow threshold set for a route pattern was violated.
AvayaSGServiceStatusOut	Out of Service: Avaya Signalling Group $sgNumber in Primary CM $hostNodeIP.	Warning	Avaya Signaling Group has become out of service.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaSuServerStatusActive	Survivable Service Active: Avaya Survibale Server ($type) with IP Address : $ipAddress and for Primary CM $cmIpAddress.	Critical	Avaya Survivable Server has become active to provide local survivability to local endpoints.
AvayaTMServiceStatusOutFE	Out of Service (far-end):Avaya Trunk member $tmNumber of Trunk Group $tgNumber of Primary CM $cmIpAddress.	Warning	Avaya Trunk Member has become out of service (far-end).
AvayaTMServiceStatusOutNE	Out of Service (near-end):Avaya Trunk member $tmNumber of Trunk Group $tgNumber of Primary CM $cmIpAddress.	Warning	Avaya Trunk Member has become out of service (near-end).
AvayaTanIncomingPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Tandem Trunk Load metric Incoming Peg = $loadtanTanIncomingPeg for measurement hour $loadtanMeasHour.	Warning	This incident is generated when the Tandem Trunk Load, Incoming Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaTanIncomingUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Tandem Trunk Load metric Incoming Use = $loadtanTanIncomingUse for measurement hour $loadtanMeasHour.	Warning	This incident is generated when the Tandem Trunk Load, Incoming Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaTanIntraPNPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Tandem Trunk Load metric Intra PN Peg = $loadtanTanIntraPNPeg for measurement hour $loadtanMeasHour.	Warning	This incident is generated when the Tandem Trunk Load, Intra PN Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaTanIntraPNUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Tandem Trunk Load metric Intra PN Use = $loadtanTanIntraPNUse for measurement hour $loadtanMeasHour.	Warning	This incident is generated when the Tandem Trunk Load, Intra PN Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
AvayaTanOutgoingPegViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Tandem Trunk Load metric Outgoing Peg = $loadtanTanOutgoingPeg for measurement hour $loadtanMeasHour.	Warning	This incident is generated when the Tandem Trunk Load, Outgoing Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaTanOutgoingUseViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber Tandem Trunk Load metric Outgoing Use = $loadtanTanOutgoingUse for measurement hour $loadtanMeasHour.	Warning	This incident is generated when the Tandem Trunk Load, Outgoing Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaTotalTDMOccViolate	Threshold breached: Avaya Primary CM: $cmIpAddress, Port Network: $pnNumber metric TDM Occupancy = $loadtotalTDMOccupancy for measurement hour $loadtotalMeasHour.	Warning	This incident is generated when the TDM Occupancy Parameter in Avaya Port Network TDM Occupancy Resource, has breached the threshold you specified for an Avaya Port Network.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
avayaMedProUnknown	Avaya Media Processor $medproName is in Unknown state in Avaya Primary CM $cmIpAddress Port network $pnNumber.	Warning	The Avaya Media Processor is in the Unknown state.
avayaMedProStandby	Avaya Media Processor $medproName is in Standby state in Avaya Primary CM $cmIpAddress Port network $pnNumber.	Warning	The Avaya Media Processor is in the Standby state.
avayaMedProInit	Avaya Media Processor $medproName is in Init state in Avaya Primary CM $cmIpAddress Port network $pnNumber.	Warning	The Avaya Media Processor is in the Init state
avayaMedProControlLinkUnknown	Control Link state is in Unknown state for Avaya Media Processor $medproName in Avaya Primary CM $cmIpAddress Port network $pnNumber.	Warning	The Avaya Media Processor Control Link is in the Unknown state
avayaMedProControlLinkDown	Control Link is Down for Avaya Media Processor $medproName in Avaya Primary CM $cmIpAddress Port network $pnNumber.	Warning	The Avaya Media Processor Control Link is in the Down state
avayaIPServerInterfaceUnknown	IPSI Service is in Unknown state: IPSI $ipsiIP in Avaya Primary CM $cmIpAddress Port network $pnNumber.	Warning	The Avaya IP Server Interface (IPSI) Service State is in the Unknown state

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
avayaIPServerInterfaceOUT	Out of Service:IPSI $ipsiIP in Avaya Primary CM $cmIpAddress Port network $pnNumber.	Warning	The Avaya IP Server Interface (IPSI) Service State is in OUT state
avayaIPNetworkRegionConnectionViolate	Threshold Breached: Avaya CM Server $cmIpAddress Network Region Connection from Network region $source to $destination Denial Connection Count = $denialCount.	Warning	The Avaya IP Network Region Denial Connection Count breached the threshold.
avayaIPNetworkRegionConnectionUnknown	Avaya Primary CM $cmIpAddress Network Region Connection from Network region $source to $destination is in Unknown state.	Warning	The Avaya IP Network Region Connection is in the Unknown state
avayaIPNetworkRegionConnectionFail	Avaya Primary CM $cmIpAddress Network Region Connection from Network region $source to $destination is in Failed state.	Warning	Avaya IP Network Region Connection is in the Failed state
ProcTotalCallsViolate	Threshold Breached: Avaya CM Server $ipAddress Total Calls Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor Total Calls Occupancy has breached the threshold specified by you on the Avaya Communication Manager

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
ProcTotalAttemptedCallsViolate	Threshold Breached: Avaya CM Server $ipAddress Total Call Attempts Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	Processor Total Call Attempts Occupancy has breached the threshold specified by you on the Avaya Communication Manager.
ProcTandemCallsViolate	Threshold Breached: Avaya CM Server $ipAddress Tandem Calls Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor Tandem Calls Occupancy has breached the threshold specified by you on the Avaya Communication Manager.
ProcSystemMgmtViolate	Threshold Breached: Avaya CM Server $ipAddress System Management Processing Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor System Management Processing Occupancy has breached the threshold specified by you on the Avaya Communication Manager.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
ProcStaticOccuViolate	Threshold Breached: Avaya CM Server $ipAddress Static Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor Static Occupancy has breached the threshold specified by you on the Avaya Communication Manager.
ProcPrivNetAttemptsViolate	Threshold Breached: Avaya CM Server $ipAddress Private Network Attempts Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor Private Network Attempts Occupancy has breached the threshold specified by you on the Avaya Communication Manager.
ProcOutCallsViolate	Threshold Breached: Avaya CM Server $ipAddress Outgoing Attempts Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor Outgoing Attempts Occupancy has breached the threshold specified by you on the Avaya Communication Manager.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
ProcIntercomCallsViolate	Threshold Breached: Avaya CM Server $ipAddress Intercom Attempts Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor Intercom Attempts Occupancy has breached the threshold specified by you on the Avaya Communication Manager.
ProcIncomingCallsViolate	Threshold Breached: Avaya CM Server $ipAddress Incoming Call Attempts Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor Incoming Call Attempts Occupancy has breached the threshold specified by you on the Avaya Communication Manager.
ProcIdleOccupancyViolate	Threshold Breached: Avaya CM Server $ipAddress Idle Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor Idle Occupancy has breached the threshold specified by you on the Avaya Communication Manager.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
ProcCallProcessingViolate	Threshold Breached: Avaya CM Server $ipAddress Call Processing Occupancy = $currentValue for measurement hour $procMeasHour.	Warning	The Processor Call Processing Occupancy has breached the threshold specified by you on the Avaya Communication Manager.
IPNetworkRegionUsageViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric Usage = $ipdspUsage for measurement hour: $dspMeasHour.	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource Usage parameter has breached the threshold value you specified for an IP Network Region.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
IPNetworkRegionPercentBlockedViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric Allocations Blocked Percentage = $pctBlocked for measurement hour: $dspMeasHour.	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource Allocations Blocked Percentage parameter has breached the threshold value you specified for an IP Network Region.
IPNetworkRegionOutSrvViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric Percentage of Out Of Service = $outOfSrv for measurement hour: $dspMeasHour.	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource Percentage of Out of Service parameter has breached the threshold value you specified for an IP Network Region.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
IPNetworkRegionG723UsageViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric G723 Usage = $codecG723Usage for measurement hour: $codecMeashour.	Warning	This incident is generated when the G723 Usage Parameter in Avaya IP Media Processor DSP Resource,has breached the threshold value you specified for an IP Network Region.
IPNetworkRegionG723OutViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric G723 Out Of Region Allocations = $codecG723OutRegion for measurement hour: $codecMeashour.	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource G723 Out Region Allocations parameter has breached the threshold value you specified for an IP Network Region.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
IPNetworkRegionG723InViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric G723 InRegion Allocations = $codecG723InRegion for measurement hour: $codecMeashour.	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource G723 In Region Allocations parameter has breached the threshold value you specified for an IP Network Region.
IPNetworkRegionG711UsageViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric G711 Usage = $codecG711Usage for measurement hour: $codecMeashour.	Warning	This incident is generated when the G711 Usage Parameter in Avaya IP Media Processor DSP Resource, has breached the threshold value you specified for an IP Network Region.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
IPNetworkRegionG711OutViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric G711 Out Of Region Allocations = $codecG711OutRegion for measurement hour: $codecMeashour.	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource G711 Out Region Allocations parameter has breached the threshold value you specified for an IP Network Region.
IPNetworkRegionG711InViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric G711 InRegion Allocations = $codecG711InRegion for measurement hour: $codecMeashour.	Warning	This incident is generated when the G711 In Region Allocations Parameter in Avaya IP Media Processor DSP Resource, has breached the threshold value you specified for an IP Network Region.

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
IPNetworkRegionDeniedViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric Allocations Denied = $dspDenied for measurement hour: $dspMeasHour.	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource Allocations Denied parameter has breached the threshold value you specified for an IP Network Region.
IPNetworkRegionDSPOutViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric Out of Region Allocations = $dspOutRegion for measurement hour: $dspMeasHour.	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource Out of Region Allocations parameter has breached the threshold value you specified for an IP Network Region

Avaya IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Avaya IP Telephony Incident	Message	Severity	Description
IPNetworkRegionDSPInViolate	Threshold Breached:Avaya Primary CM $cmIpAddress Network Region $number CODEC/DSP resources metric InRegion Allocations = $dspInRegion for measurement hour: $dspMeasHour.	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource In Region Allocations parameter has breached the threshold value you specified for an IP Network Region

Cisco IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony

Cisco IP Telephony Incident	Message	Severity	Description
LowQOSCall	$18; $19; $20; $21; $22 for call from $callingPartyNumber to $finalCalledPartyNumber, from device: $origDeviceName to device: $destDeviceName in Cluster: $globalCallIdClusterId.	Critical	This incident indicates a low voice quality call between two given phones, along with their extension and IP address details, cluster-Id of the source phone, and QoS details (such as Jitter, Latency, and average MOS).

Cisco IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Cisco IP Telephony Incident	Message	Severity	Description
CiscoCktSwitchedIFStatusIdle	Cisco Circuit Switched interface $cktSwitchedIfName Usage state is Unknown. Gateway $gwIPAddress.	Warning	This incident indicates that the usage state of a circuit switched interface (the endpoint hosted on a voice gateway) has changed to idle. The usage state of an endpoint is computed by considering the usage state of the bearer channels for the endpoint.
CiscoCktSwitchedIFOperStatusDown	Cisco Circuit Switched interface $cktSwitchedIfName Operational state is Critical. Gateway $gwIPAddress.	Warning	This incident indicates that the operational state of a circuit switched interface (endpoint) hosted on a voice gateway has changed from up to down.
CiscoCallManagerStatusDown	UCOS CallManager service is possibly down in CUCM with IP: $ip in Cluster: $cluster; Subscriber Group (CUCM Priority): $cmGrpAndPriority.	Critical	This incident indicates that the Unified Communications Operating System (UCOS) CallManager service is down.

Cisco IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Cisco IP Telephony Incident	Message	Severity	Description
CiscoCktSwitchedIFRegnStatusUnReg	Cisco Circuit Switched interface $cktSwitchedIfName Registration state is Unregistered. Gateway $gwIPAddress Cluster $cluster.	Warning	This incident indicates that the registration state of a circuit switched interface (endpoint) hosted on a voice gateway has changed from registered to unregistered.
CiscoCktSwitchedIFRegnStatusRejected	Cisco Circuit Switched interface $cktSwitchedIfName Registration state is Rejected. Gateway $gwIPAddress Cluster $cluster.	Warning	This incident indicates that the registration state of a circuit switched interface (endpoint) hosted on a voice gateway has changed to rejected. It happens when a call manager rejects an interface register request.
CiscoCktSwitchedIFRegnStatusUnknown	Cisco Circuit Switched interface $cktSwitchedIfName Registration state is Unknown. Gateway $gwIPAddress Cluster $cluster.	Warning	This incident indicates that the registration state of a circuit switched interface (endpoint hosted on a voice gateway) has changed to unknown.

Cisco IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Cisco IP Telephony Incident	Message	Severity	Description
CiscoPhoneUnRegistered	Cisco IP Phone Unregistered in Cluster: $cluster.	Warning	Cisco Phone Unregistered from a Cisco CallManager.
CiscoPhoneDeceased	Cisco IP Phone Deceased	Warning	The Cisco IP Phone configured to register with the SRST in fall-back mode has deceased
CiscoSrstActive	Cisco SRST $ip Active in Cluster $cluster.	Critical	The Cisco SRST is in the active state.
CiscoVMDeviceRejected	Cisco Voice Mail Device $vmName in Cluster $cluster is in Rejected state.	Warning	The Cisco Voice Mail Device has changed its state to Rejected
CiscoVMDeviceUnknown	Cisco Voice Mail Device $vmName in Cluster $cluster is in Unknown state.	Warning	The Cisco Voice Mail Device has changed its state to Unknown
CiscoVMDeviceUnregistered	Cisco Voice Mail Device $vmName in Cluster $cluster is in Unregistered state.	Warning	The Cisco VM Device is in the unregistered state.

Cisco IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Cisco IP Telephony Incident	Message	Severity	Description
CiscoGkControlledICTStatusRejected	The Gatekeeper-Controlled Inter-Cluster Trunk: $trunkName in Cluster: $clusterId is in Rejected state.	Warning	This incident is generated whenever a Gatekeeper-Controlled Inter-Cluster Trunk's registration request is rejected by a Cisco CallManager.
CiscoGkControlledICTStatusUnRegd	The Gatekeeper-Controlled Inter-Cluster Trunk: $trunkName in Cluster: $clusterId is in UnRegistered state.	Warning	This incident is generated when ever a Gatekeeper-Controlled Inter-Cluster Trunk un registers with a call manager.
CiscoVgwStatusCritical	Cisco Voice Gateway Status is Critical. Gateway IP Address: $ipAddress	Critical	Cisco Voice Gateway Status is Critical.
CiscoVgwStatusWarning	Cisco Voice Gateway Status is Warning. Gateway IP Address: $ipAddress	Warning	Cisco Voice Gateway Status is Warning.
CiscoVgwStatusMinor	Cisco Voice Gateway Status is Minor. Gateway IP Address: $ipAddress	Minor	Cisco Voice Gateway Status is Minor.

Cisco IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Cisco IP Telephony Incident	Message	Severity	Description
CallTerminationReason	Termination reason is "$terminationReason" for call from $callingPartyNumber to $finalCalledPartyNumber in Cluster $clusterId from device "$origEndpointName" to device "$destEndpointName".	Warning	This incident is generated when the user-specified call termination cause code to be monitored, matches with a call termination cause code.
MonitoredAttributeThresholdBreachCrirtical	$messageFormat	Critical	This incident is generated with Critical incident severity when the monitored attribute exceeds the critical threshold value that you specified.
MonitoredAttributeThresholdBreachMajor	$messageFormat	Major	This incident is generated with Major incident severity when the monitored attribute exceeds the critical threshold value that you specified.

Cisco IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Cisco IP Telephony Incident	Message	Severity	Description
MonitoredAttributeThresholdBreachMinor	$messageFormat	Minor	This incident is generated with Minor incident severity when the monitored attribute exceeds the critical threshold value that you specified.
MonitoredAttributeThresholdBreachWarning	$messageFormat	Warning	This incident is generated with Warning incident severity when the monitored attribute exceeds the critical threshold value that you specified.

Microsoft IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony

Microsoft IP Telephony Incident	Message	Severity	Description	
MSProxyDisconnected	Microsoft proxy connection to $proxyAddress on port $proxyPort is DOWN.	Critical	This incident indicates that the connection between the NNM iSPI for IP Telephony and Microsoft proxy (MS IPT Proxy), which runs at the specified IP address and port, is down.	

Microsoft IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

MSProxyConnected	Microsoft proxy connection to $proxyAddress on port $proxyPort is UP.	Normal	This incident indicates that the connection between the NNM iSPI for IP Telephony and Microsoft proxy (MS IPT Proxy), which runs at the specified IP address and port, is up. The NNM iSPI for IP Telephony generates this incident to close the *MSProxyDisconnected* incident.	
MSProxyCollectionFailure	Microsoft proxy $proxyName failed to collect data from Front End pool $target	Major	This incident indicates that the particular Microsoft proxy (MS IPT Proxy) has failed in collecting data from the specified front end server pool.	
MSProxyCollectionSuccess	Microsoft proxy $proxyName successfully collected data from the Front End pool $target.	Normal	This incident indicates that the named Microsoft proxy instance has successfully collected data from the specified front end server pool. The NNM iSPI for IP Telephony generates this incident to close the *MSProxyCollectionFailure* incident.	
GatewayOperStatusDown	The operational state of Gateway: $gwIdentity has changed to critical. Gateway ipaddress: $gwIPAddress	Critical	This incident indicates that operational state of all gateway interface i.e. endpoints hosted on the gateway has changed to down.	

Microsoft IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

GatewayInterfaceOperStatusDown	The operational state of Gateway interface: $ifaceName has changed to critical. Gateway ipaddress: $gwIPAddress	Critical	This incident indicates that the operational state of a gateway interface—the endpoint hosted on a voice gateway—has changed from up to down.	
GatewayInterfaceLineStatusAlarmed	Line Alarms(s) active on Gateway Interface: <gateway interface name> in Gateway: <IP Address of the Gateway>	Critical	This incident indicates that there are active alarm (s) on a gateway interface—the endpoint hosted on a voice gateway.	
GatewayInterfaceStatusIdle	Usage state of Gateway interface: <Gateway interface name> has changed to critical. Gateway ip address: <IP Address of the Gateway>	Critical	This incident indicates that the usage state of a gateway interface i.e. endpoint hosted on a voice gateway has changed to idle. The NNM iSPI for IP Telephony closes the incident as soon as the interface state changes from `Idle` to `Connected` or `Partially Used`. For more information, see Gateway Channel Incident.	
GatewayChannelStatusIdle	Channel: *$chName* was found in Idle state for configured Idle Time. Gateway ipaddress: *$gwIPAddress*	Critical	Gateway channel usage status is idle.	

Nortel IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony

Nortel IP Telephony Incident	Message	Severity	Description
callsMadeInViolation	The Intra QOS Zone callsMadeIn parameter has violated set threshold value.	Critical	The Intra QOS Zone callsMadeIn parameter has violated set threshold value.
callsMadeOutViolation	The Inter QOS Zone callsMadeOut parameter has violated set threshold value.	Critical	The Inter QOS Zone callsMadeOut parameter has violated set threshold value.
callsBlockedOutViolated	The Inter QOS Zone callsBlockedOut parameter has violated set threshold value.	Critical	The Inter QOS Zone callsBlockedOut parameter has violated set threshold value.
callsPeakInViolated	The Intra QOS Zone peakIn parameter has violated set threshold value.	Critical	The Intra QOS Zone peakIn parameter has violated set threshold value.
callsBlockedInViolated	The Intra QOS Zone callsBlockedIn parameter has violated set threshold value.	Critical	The Intra QOS Zone callsBlockedIn parameter has violated set threshold value.
callsPeakOutViolated	The Inter QOS Zone peackOut parameter has violated set threshold value.	Critical	The Inter QOS Zone peackOut parameter has violated set threshold value.
inThrViolViolated	The Intra QOS Zone inThrViol parameter has violated set threshold value	Critical	The Intra QOS Zone inThrViol parameter has violated set threshold value.
outThrViolViolated	The Inter QOS Zone outThrViol parameter has violated set threshold value.	Critical	The Inter QOS Zone outThrViol parameter has violated set threshold value.
avgInViolated	The Intra QOS Zone avgIn parameter has violated set threshold value.	Critical	The Intra QOS Zone avgIn parameter has violated set threshold value.

Nortel IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Nortel IP Telephony Incident	Message	Severity	Description
avgOutViolated	The Inter QOS Zone avgOut parameter has violated set threshold value.	Critical	The Inter QOS Zone avgOut parameter has violated set threshold value.
unacpLatencyInViolated	The Intra QOS Zone unacpLatencyIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpLatencyIn parameter has violated set threshold value.
intervalOutViolated	The Inter QOS Zone intervalOut parameter has violated set threshold value.	Critical	The Inter QOS Zone intervalOut parameter has violated set threshold value.
intervalInViolated	The Intra QOS Zone intervalIn parameter has violated set threshold value.	Critical	The Intra QOS Zone intervalIn parameter has violated set threshold value.
unacpLatencyOutViolated	The Inter QOS Zone unacpLatencyOut parameter has violated set threshold value.	Critical	The Inter QOS Zone unacpLatencyOut parameter has violated set threshold value.
unacpPacketLossInViolated	The Intra QOS Zone unacpPacketLossIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpPacketLossIn parameter has violated set threshold value.
unacpPacketLossOutViolated	The Inter QOS Zone unacpPacketLossOut parameter has violated set threshold value.	Critical	The Inter QOS Zone unacpPacketLossOut parameter has violated set threshold value.
unacpRFactorInViolated	The Intra QOS Zone unacpRFactorIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpRFactorIn parameter has violated set threshold value.

Nortel IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Nortel IP Telephony Incident	Message	Severity	Description
unacpJitterOutViolated	The Inter QOS Zone unacpJitterOut parameter has violated set threshold value.	Critical	The Inter QOS Zone unacpJitterOut parameter has violated set threshold value.
unacpJitterInViolated	The Intra QOS Zone unacpJitterIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpJitterIn parameter has violated set threshold value.
unacpRFactorOutViolated	The Inter QOS Zone unacpRFactorOut parameter has violated set threshold value.	Critical	The Inter QOS Zone unacpRFactorOut parameter has violated set threshold value.
unacpEchoRLossOutViolated	The Inter QOS Zone unacpEchoRLossOut parameter has violated set threshold value	Critical	The Inter QOS Zone unacpEchoRLossOut parameter has violated set threshold value.
unacpEchoRLossInViolated	The Intra QOS Zone unacpEchoRLossIn parameter has violated set threshold value.	Critical	The Intra QOS Zone unacpEchoRLossIn parameter has violated set threshold value.
warnPacketLossInViolated	The Intra QOS Zone warnPacketLossIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnPacketLossIn parameter has violated set threshold value.
warnLatencyOutViolated	The Inter QOS Zone warnLatencyOut parameter has violated set threshold value.	Critical	The Inter QOS Zone warnLatencyOut parameter has violated set threshold value.
warnLatencyInViolated	The Intra QOS Zone warnLatencyIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnLatencyIn parameter has violated set threshold value.

Nortel IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Nortel IP Telephony Incident	Message	Severity	Description
warnRFactorInViolated	The Intra QOS Zone warnRFactorIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnRFactorIn parameter has violated set threshold value.
warnJitterOutViolated	The Inter QOS Zone warnJitterOut parameter has violated set threshold value.	Critical	The Inter QOS Zone warnJitterOut parameter has violated set threshold value.
warnEchoRLossInViolated	The Intra QOS Zone warnEchoRLossIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnEchoRLossIn parameter has violated set threshold value.
warnEchoRLossOutViolated	The Inter QOS Zone warnEchoRLossOut parameter has violated set threshold value.	Critical	The Inter QOS Zone warnEchoRLossOut parameter has violated set threshold value.
warnRFactorOutViolated	The Inter QOS Zone warnRFactorOut parameter has violated set threshold value.	Critical	The Inter QOS Zone warnRFactorOut parameter has violated set threshold value.
warnJitterInViolated	The Intra QOS Zone warnJitterIn parameter has violated set threshold value.	Critical	The Intra QOS Zone warnJitterIn parameter has violated set threshold value.
warnPacketLossOutViolated	The Inter QOS Zone warnPacketLossOut parameter has violated set threshold value.	Critical	The Inter QOS Zone warnPacketLossOut parameter has violated set threshold value.

Nortel IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Nortel IP Telephony Incident	Message	Severity	Description
NortelISetStatusUnregistered	Nortel IP Phone Unregistered. Extension: $extension. Signaling Server: $ssIpAddress. Call Server: $controllerIpAddress	Minor	The Nortel IP Phone is in the unregistered.state.
commonMIBAlarmMinor	Minor alarm condition on Nortel device $6. Err Code $7. Alarm Type $8. Probable Cause $9. Alarm Data $10.	Critical	This trap is used to provide a real time indication of a minor alarm condition. The variables listed in VARIABLES clause are defined in `mgmt-info`group and are present in all information alarms.
commomMIBAlarmCritical	Critical alarm condition on Nortel device $6. Err Code $7. Alarm Type $8. Probable Cause $9. Alarm Data $10.	Critical	This trap is used to provide a real time indication of a critical alarm condition. The variables listed in VARIABLES clause are defined in the `mgmt-info` group and are present in all information alarms.
commonMIBAlarmClear	Clear alarm condition on Nortel device $6. Err Code $7. Alarm Type $8. Probable Cause $9. Alarm Data $10.	Normal	This trap is used to provide a real time indication of a clear alarm condition. The variables listed in VARIABLES clause are defined in `mgmt-info` group and are present in all information alarms.

Nortel IP Telephony - Incidents Generated by the NNM iSPI for IP Telephony, continued

Nortel IP Telephony Incident	Message	Severity	Description
commonMIBAlarmIndeterminate	Indeterminate alarm condition on Nortel device $6. Err Code $7. Alarm Type $8. Probable Cause $9. Alarm Data $10.	Normal	This trap is used to provide a real time indication of an indeterminate alarm condition. The variables listed in VARIABLES clause are defined in `mgmt-info` group and are present in all information alarms.
commonMIBAlarmInfo	Informational alarm condition on Nortel device $6. Err Code $7. Alarm Type $8. Probable Cause $9. Alarm Data $10.	Normal	This trap is used to provide a real time indication of an information alarm condition. The variables listed in VARIABLES clause are defined in `mgmt-info` group and are present in all information alarms.
commonMIBAlarmMajor	Major alarm condition on Nortel device $6. Err Code $7. Alarm Type $8. Probable Cause $9. Alarm Data $10.	Major	This trap is used to provide a real time indication of a major alarm condition. The variables listed in VARIABLES clause are defined in `mgmt-info` group and are present in all information alarms.
commonMIBAlarmWarning	Warning alarm condition on Nortel device $6. Err Code $7. Alarm Type $8. Probable Cause $9. Alarm Data $10.	Warning	This trap is used to provide a real time indication of a warning alarm condition. The variables listed in VARIABLES clause are defined in `mgmt-info` group and are present in all information alarms.

View SNMP Traps for Avaya Maintenance Objects

The NNM iSPI for IP Telephony can receive select SNMP traps that originate from Avaya maintenance objects (MOs) and are defined in the G3-Avaya-MIB.These traps are visible in the

Incident View of the NNMi console. The NNM iSPI for IP Telephony can receive traps from the following MOs and show the them in the Incident View:

- Control LAN Circuit Pack
- Control LAN Ethernet
- Control LAN Packet/Port
- IP Media Processor
- IP Media Processor DSP port
- IP Media Processor MAPD Circuit Pack
- Media Gateway/ Common Media Gateway
- IP Server Interface
- Survivable Processor
- Survivable Processor-Main

The NNM iSPI for IP Telephony receives only the following types of traps that originate from Avaya MOs:

- alarmMajor
- alarmMinor
- alarmWarning
- alarmResolved

In addition, the NNM iSPI for IP Telephony generates Root Cause Incidents for specific Avaya MOs based on the SNMP traps received from those MOs.

Incidents for Avaya Devices

The NNM iSPI for IP Telephony generates incidents for the following Avaya devices based on SNMP traps that it receives from Avaya MOs :

- Control LAN
- IP media processor
- IP server interface
- Avaya Communication Manager (primary or survivable server)
- Media gateway

The NNM iSPI for IP Telephony first determines the state of each MO (specified in Types of Avaya MO SNMP Trap) from the received SNMP trap, and then generates an incident for a device if at least one underlying MO for the device has the status Major, Minor, or Warning. Table: Underlying MOs for Monitored Avaya Devices lists the underlying MOs for each device.

Table: Underlying MOs for Monitored Avaya Devices

Device Type	Underlying MOs
Control LAN	• Control LAN Circuit Pack • Control LAN Ethernet • Control LAN Packet/Port
IP media processor	• IP Media Processor • IP Media Processor DSP port • IP Media Processor MAPD Circuit Pack
IP server interface	IP Server Interface
Media gateway	Media Gateway/ Common Media Gateway
Avaya Communication Manager	• Processor • Processor-Main

To calculate the severity of each incident, the NNM iSPI for IP Telephony uses the following rules:

- If the status of at least one MO is Major, the severity of the incident is Major.
- If no MO is of the status Major and the status of at least one MO is Minor, the severity of the incident is Minor.
- If no MO is of the status Major or Minor and the status of at least one MO is Warning, the severity of the incident is Warning.

The NNM iSPI for IP Telephony can preserve the state of every monitored Avaya MO in the event of iSPI or NNMi downtime.After the NNM iSPI for IP Telephony starts up again, the old states are displayed for Avaya MOs until the next polling cycle.

Viewing Network Connectivity

With the NNM iSPI for IP Telephony, you can view the complete connectivity of the IP telephony network that you want to monitor. NNMi enables you to monitor the complete topology of the discovered network. If you log on to the NNMi console with operator (level 1 or level 2) or guest credentials, you can use the following tools to view the complete overview of your IP telephony network:

- **Topology Maps**

  The Topology Maps workspace of NNMi will help you view the complete topology of the IP telephony network. With the help of the following maps, you can perform a diagnosis of the connectivity between the devices in the IP telephony network.

  - Network Overview
  - Networking Infrastructure Devices
  - Routers
  - Switches

- **Troubleshooting**

  The Troubleshooting workspace helps you launch the path view, layer 2 neighbor view, or layer 3 neighbor view . These views help you identify the devices (layer 2 or 3) that reside between two different IP telephony devices.

  See the *NNMi Online Help for Operators* for more information on these views.

- **IP Telephony Maps:**

  The NNM iSPI for IP Telephony presents the following additional map views for diagnosing specific problems in the IP telephony environment:

  > **Tip:** To view these views, you must log on to the NNMi console as operator 1, operator 2, guest, or administrator.

  - Voice path
  - Control path
  - HTTP to Phone path (this feature is not available for Cisco)
  - Voice Quality: Graph Average MOS
  - Voice Quality: Graph Average Packet Loss
  - Voice Quality: Graph Jitter
  - Voice Quality: Graph Latency
  - Network Flow Reports (available only if you install the NNM iSPI Performance for Traffic)
  - QA Report for Voice Path (available only if you install the NNM iSPI Performance for QA)

Viewing the Graph for Jitter

With the NNM iSPI for IP Telephony, you can launch the line graph to show the jitter in milliseconds between two Cisco IP phones or two active Avaya IP phones. The report displays the jitter for the calls between the two selected phones.

Note: The **File** > **Export to CSV** option is not supported for this graph.

To launch the graph to view the jitter for Cisco IP phones, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.
2. In the Cisco IP Phones view, select two different Cisco IP phones.
3. Click **Actions > IP Telephony > Voice Quality: Graph Jitter**. Alternatively, right-click a Cisco IP phone, and then click **IP Telephony** > **Voice Quality: Graph Jitter**. The line graph opens in a new window.

To launch the graph to view the jitter for active Avaya IP phones, follow these steps:

1. From the **Workspaces** navigation pane, click **Avaya IP Telephony** > **Avaya IP Phones**. The Avaya IP Phones view opens in the right pane.
2. From the Avaya IP Phones view, select an active Avaya IP phone.
3. Click **Actions > IP Telephony > Voice Quality: Graph Jitter**. Alternatively, right-click an active Avaya IP phone, and then click **IP Telephony** > **Voice Quality: Graph Jitter**. The **Active RTP Sessions** page opens.
4. Select the CNAME for which you want to launch the voice graph, and then click (the **Launch Voice Graph** icon). The line graph opens in a new window.

Viewing the Graphs for Average Packet Loss

With the NNM iSPI for IP Telephony, you can launch the line graph to show the percentage of the average packet loss between two Cisco IP phones or two Avaya IP phones. The report displays the percentage of the packet loss for the calls between the two selected phones.

Note: The **File** > **Export to CSV** option is not supported for this graph.

To launch the graph to view the average packet loss between two Cisco IP phones, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony** > **Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.

2. In the Cisco IP Phones view, select two different Cisco IP phones.

3. Click **Actions > IP Telephony > Voice Quality: Graph Average Packet Loss**. Alternatively, right-click a Cisco IP phone, and then click **IP Telephony** > **Voice Quality: Graph Average Packet Loss**. The line graph opens in a new window.

To launch the graph to view the average packet loss between two Avaya IP phones, follow these steps:

1. From the **Workspaces** navigation pane, click **Avaya IP Telephony** > **Avaya IP Phones**. The Avaya IP Phones view opens in the right pane.

2. From the Avaya IP Phones view, select an active Avaya IP phone.

3. Click **Actions > IP Telephony > Voice Quality: Graph Average Packet Loss**. Alternatively, right-click an active Avaya IP phone, and then click **IP Telephony** > **Voice Quality: Graph Average Packet Loss**. The **Active RTP Sessions** page opens.

4. Select the CNAME for which you want to launch the voice graph, and then click (the **Launch Voice Graph** icon). The line graph opens in a new window.

Viewing the Graph for the Average MOS

With the NNM iSPI for IP Telephony, you can launch the line graph to show the average Mean Opinion Score (MOS) between two Cisco IP phones or two Avaya IP phones. The report displays the MOS for the calls between the two selected phones.

Note: The **File** > **Export to CSV** option is not supported for this graph.

To launch the graph to view the average MOS between two Cisco IP phones, follow these steps:

1. From the **Workspaces** navigation pane, click **CiscoIP Telephony** > **Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.

2. In the Cisco IP Phones view, select two different Cisco IP phones.

3. Click **Actions > IP Telephony > Voice Quality: Graph Average MOS**. Alternatively, right-click a Cisco IP phone, and then click **IP Telephony** > **Voice Quality: Graph Average MOS**. The line graph opens in a new window.

To launch the graph to view the average MOS between two Avaya IP phones, follow these steps:

1. From the **Workspaces** navigation pane, click **Avaya IP Telephony** > **Avaya IP Phones**. The Avaya IP Phones view opens in the right pane.

2. From the Avaya IP Phones view, select an active Avaya IP phone.

3. Click **Actions > IP Telephony > Voice Quality: Graph Average MOS**. Alternatively, right-click an active Avaya IP phone, and then click **IP Telephony** > **Voice Quality: Graph Average MOS**. The **Active RTP Sessions** page opens.

4. Select the CNAME for which you want to launch the voice graph, and then click (the **Launch Voice Graph** icon). The line graph opens in a new window.

Viewing the Graphs for Latency

With the NNM iSPI for IP Telephony, you can launch the line graph to show the latency in milliseconds between two Cisco IP phones or two , Avaya IP phones. The report displays the latency for the calls between the two selected phones.

Note: The **File** > **Export to CSV** option is not supported for this graph.

To launch the graph to view the latency between two Cisco IP phones, follow these steps:

1. From the **Workspaces** navigation pane, click **CiscoIP Telephony** > **Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.

2. In the Cisco IP Phones view, select two different Cisco IP phones.

3. Click **Actions > IP Telephony > Voice Quality: Graph Latency**. Alternatively, right-click a Cisco IP phone, and then click **IP Telephony** > **Voice Quality: Graph Latency**. The line graph opens in a new window.

To launch the graph to view the latency between two Avaya IP phones, follow these steps:

1. From the **Workspaces** navigation pane, click **Avaya IP Telephony** > **Avaya IP Phones**. The Avaya IP Phones view opens in the right pane.

2. From the Avaya IP Phones view, select an active Avaya IP phone.

3. Click **Actions > IP Telephony > Voice Quality: Graph Latency**. Alternatively, right-click an active Avaya IP phone, and then click **IP Telephony** > **Voice Quality: Graph Latency**. The **Active RTP Sessions** page opens.

4. Select the CNAME for which you want to launch the voice graph, and then click (the **Launch Voice Graph** icon). The line graph opens in a new window.

Launch a Voice Path

With the NNM iSPI for IP Telephony, you can launch the voice path between two Cisco or Avaya IP phones. You can launch a voice path graph even if you have not seeded IP Phones in NNMi. The voice path graph displays all the layer 2 and 3 devices between two IP phones with all the associated interfaces. The graphs presents an easy way to view the states of the connecting IP phones, all the intermediate layer 2/3 devices, and associated interfaces.

If you configured multiple tenant objects, make sure that the following tasks are complete before launching the voice path:

- Overlapping IP addresses are mapped for each Cisco IP phone
- Overlapping IP addresses for all elements in an Avaya C-LAN are mapped

To launch a voice path view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.
2. In the Cisco IP Phones view, select two different Cisco IP phones.
3. Click **Actions > IP Telephony > Voice Path**. The voice path graph opens in a new window.

Note: You can follow the steps listed and select the workspace and the IP phones for Avaya IP phones; select two Avaya IP phones to launch the voice path between the Avaya phones.

By default, the NNM iSPI for IP Telephony launches the path between the phone that you selected first and the phone that you selected second, which is referred to as the forward path. You can do as follows to launch the reverse path from the phone you chose second to the phone you chose first:

1. Click the **Forward Path** drop-down list
2. Select **Reverse Path**
3. Click the **Compute Path** icon adjacent to the drop-down list

Launch a Control Path

A control path displays the connectivity between an IP phone and the controlling CallManager (for Cisco) or the primary server (for Avaya). You can launch a control path graph even if you have not seeded IP Phones in NNMi. The control path graph displays all the layer 2 and 3 devices between the IP phone and the call controller with all the associated interfaces. The graphs presents an easy way to view the states of all the intermediate layer 2/3 devices and associated interfaces.

If you configured multiple tenant objects, make sure that the following tasks are complete before launching the control path:

- Overlapping IP addresses are mapped for each Cisco IP phone
- Overlapping IP addresses for all elements in an Avaya C-LAN are mapped

To launch a control path view, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.

2. In the Cisco IP Phones view, select a Cisco IP phone.
3. Click **Actions > IP Telephony > Control Path**. The control path graph opens in a new window.

Note: You can follow the steps listed and select the workspace and the Avaya IP phone to launch the control path for the selected IP phone.

By default, the NNM iSPI for IP Telephony launches the path between the phone and the call controller, which is referred to as the forward path. You can do as follows to launch the reverse path from the phone to the call controller as follows:

1. Click the **Forward Path** drop-down list
2. Select **Reverse Path**
3. Click the **Compute Path** icon adjacent to the drop-down list

Launch the HTTP to Phone Path

The HTTP to Phone path view displays the configuration information page for the selected Cisco IP phone.

To launch the HTTP to Phone path for a Cisco IP Phone, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.
2. In the Cisco IP Phones view, select a Cisco IP phone.
3. Click **Actions > IP Telephony > HTTP to Phone**. The HTTP to Phone path view opens in a new window.

The view displays the following information for the selected Cisco IP phone:

- Device information details
- Network configuration details
- Network statistics
- Device logs
- Change configuration screens for the following parameters:
  - Network
  - Tone

- Audio

- Streaming statistics

Note: You can launch the HTTP to Phone path only for Cisco phones.

Integration with the iSPI Performance for Quality Assurance

The NNM iSPI for IP Telephony integrates with the iSPI Performance for Quality Assurance to provide you a report on the Cisco IP Service Level Agreement (IP SLA) IP SLA test results for the voice path between the selected IP phones. The integration allows you to see the IP SLA test result reports for all the Cisco IOS routers which are present in the voice path between any arbitrary pair of IP Phones. Note that the applicable routers or tests are only for the routers that have IP SLA tests configured and discovered by the iSPI Performance for Quality Assurance. For information on how to enable this optional integration between NNM iSPI for IP Telephony and iSPI Performance for Quality Assurance, see the *NNM iSPI for IP Telephony Installation Guide*.

To launch the QA report for voice path, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.
2. In the Cisco IP Phones view, select two Cisco IP phones.
3. Click **Actions > IP Telephony > QA Report for Voice Path**. The QA report for voice path view opens in a new window.

Note: You can launch the QA report for voice path only for Cisco IP phones.

Integration with the iSPI Performance for Traffic

The NNM iSPI for IP Telephony integrates with the iSPI Performance for Traffic to provide you a report on the network flow for the voice path between the selected IP phones. This report displays the following details:

- The type of traffic
- The source and the destination IP address of the selected phones
- The router interface

To launch the Network Flow report for voice path, follow these steps:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Cisco IP Phones**. The Cisco IP Phones view opens in the right pane.
2. In the Cisco IP Phones view, select two Cisco IP phones.
3. Click **Actions > IP Telephony > Network Flow Reports**. The Network Flow report for voice path view opens in a new window.

Note: You can launch the Network Flow report for voice path for Avaya IP phones by selecting the respective IP phones from the corresponding IP phone inventory view.

Chapter 5: Help for Administrators

As an administrator, you can configure the NNM iSPI for IP Telephony according to your monitoring requirements for the IP telephony devices and services on the network. You can gain access to the configuration forms presented by the NNM iSPI for IP Telephony, which help you to change the following settings:

- Exclude IP Phones that you do not want to monitor for Cisco and Avaya
- Interval for various NNM iSPI for IP Telephony monitoring tasks
- QOS and MOS monitoring threshold configuration
- Reporting configuration
- Data access configuration
- Regional Manager configuration

HP recommends that you configure the settings listed above before you seed any IP Telephony nodes in NNMi and start to monitor these nodes using the NNM iSPI for IP Telephony. However, you can use the configuration forms to configure the settings or modify the existing settings even after seeding the IP Telephony nodes or when the NNM iSPI for IP Telephony is operational.

To launch the IP Telephony Configuration forms, follow these steps:

From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration**. The NNM iSPI for IP Telephony window appears.

> **Note:** You can click the **Go back to iSPI for IP Telephony Configuration Home** link present on all the configuration forms to return back to the NNM iSPI for IP Telephony window.

The NNM iSPI for IP Telephony Quick Start Configuration Wizard

You can also run the **NNM iSPI for IP Telephony Quick Start Configuration Wizard** to configure the settings to manage your network environment. HP recommends that you use the **NNM iSPI for IP Telephony Quick Start Configuration Wizard** for the initial configuration setup.

To access the quick start wizard, type the following URL in your browser:

http://<fqdn>:<port>/iptquickstart/wizard

<*fqdn*>: The fully qualified domain name of the NNMi management server

<*port*>: The HTTP port number used by the NNM iSPI for IP Telephony. The default port number is 10080.

By default, the NNM iSPI for IP Telephony Quick Start Wizard is configured to use the credential-based authentication. However, you can configure the Quick Start Wizard to use the PKI-based authentication.

Configuring Quick Start Wizard to use PKI-based authentication

To configure the NNM iSPI for IP Telephony Quick Start Wizard to use the PKI-based authentication, follow these steps:

1. Log on to the NNM iSPI for IP Telephony server.
2. Navigate to the following directory:
   On Windows
   `%nnmdatadir%\nmsas\ipt\conf`

   On Linux
   `/var/opt/OV/nmsas/ipt/conf`
3. Open the `nms-auth-config.xml` file with a text editor.
4. Locate the following lines of code:
   ```
   <realm name="console">
   <mode>X509</mode>
   </realm>
   ```
5. Add the following lines of code after the above code:
   ```
   <realm name="iptqswrealm">
   <mode>X509</mode>
   </realm>
   ```
6. Save and close the file.
7. Run the following command at the command prompt:
   On Windows
   `%nnminstalldir%\bin\nmsiptauthconfigreload.ovpl`

   On UNIX/Linux
   `/opt/OV/bin/nmsiptauthconfigreload.ovpl`

Clarus IPC

As an administrator you can enable or disable integration of the NNM iSPI for IP Telephony with Clarus IPC to view the Clarus IPC generated traps that convey alerts for the Cisco IP Telephony service test results and configuration changes. The integration with Clarus IPC also allows you to launch the **Remote Hand** and **Help Desk** applications from Clarus IPC for certain Cisco IP Phones from the NNM iSPI for IP Telephony IP Phone view for Cisco IP phones. For more information on enabling this integration, see Integrate the iSPI Telephony with Clarus IPC.

Related Topics:

- Manage Discovery and Monitoring
- Delete IP Telephony Devices

- Enable Log File Tracing
- Integrate the iSPI Telephony with Clarus IPC

Acme IP Telephony

As an administrator, you can configure attributes listed in the table given here for monitoring the Acme IP telephony infrastructure discovered on the network.

To access the administration console, follow these steps:

1. Log on to the NNMi console as an administrator.
2. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration** > **Acme Configuration**. The administration console for Acme IP telephony appears.

The administration console displays configuration options for the following attributes:

Attribute	Description
Call Monitoring	Allows you to configure the call monitoring options of Acme IP Telephony devices. You can also use this option to view the existing call monitoring configurations.
Data Access	Allows you to configure the NNM iSPI for IP Telephony to access the various categories of management data from the Acme IP Telephony servers in your deployment environment. You can also use this option to view the existing data access configurations.
Polling	Allows you to configure the polling options of Acme IP Telephony device states and statistics. You can also use this option to view the existing polling configurations.
Reporting	Allows you to configure the Call Details Record (CDR) reports for the Acme IP Telephony network. You can also use this option to view the existing reporting configuration.

Configuring Call Monitoring

You can use the NNM iSPI for IP Telephony Acme Call Monitoring Configuration form to configure the following:

- Monitor the voice QOS metrics and MOS values for calls in the Acme IP Telephony network
- The termination cause codes that need to be monitored for a specific call in the Acme IP Telephony network

Configuring the QOS/MOS Threshold Values for Call Monitoring

The **Call Monitoring Configuration** link on the **Acme Configuration** pane enables you to configure the monitoring of voice QOS metrics and MOS values for calls in the Acme IP Telephony network. The **Thresholds for QOS/MOS Monitoring** tab on the NNM iSPI for IP Telephony Acme Call Monitoring Configuration form allows you to specify the threshold values. On violation of set threshold for any of these parameters for any monitored call, the NNM iSPI for IP Telephony generates an incident conveying the resulting values and the set threshold.

To configure the QOS/MOS monitoring threshold values for Acme IP telephony calls, follow these steps:

1. On the NNM iSPI for IP Telephony Acme Configuration console, click **Call Monitoring Configuration**. The NNM iSPI for IP Telephony Acme Call Monitoring Configuration form opens.

2. Click the **Thresholds for QOS/MOS Monitoring** tab. The Thresholds for QOS/MOS Monitoring tab page opens.

3. Specify the required details in the fields provided under the **Thresholds for QOS/MOS Monitoring** section of the page. The following table describes the fields that appear in the section:

   Tip: By default, no threshold values are set for these parameters and threshold-based monitoring is disabled. You can enable monitoring and incident generation when you specify the valid threshold values.

QOS/MOS Monitoring Parameter	Description
[1]Jitter	The jitter threshold (in milliseconds) to be configured.
[1]PPL	The Percentage Packet Loss (PPL) threshold to be configured. For example, to specify a percentage packet loss threshold of 50%, type 50.
[1]Latency	The latency (in milliseconds) threshold to be configured.
[1]RFactor	The QoS R-Factor (in percentage) to be configured. This value must be within the range of 0 to 100.
[1]Avg MOS	The average Mean Opinion Source (MOS) value to be configured. This value must be within the range of 0.0 to 5.0.

   [1]To disable the monitoring, specify **-1.0**.

4. Click **Apply Changes**. The NNM iSPI for IP Telephony updates the QOS/MOS monitoring configuration values.

Configuring Session Director—specific QOS and MOS Threshold Values

The **Add Session Director Specific QOS Configuration** section on the **Thresholds for QOS/MOS Monitoring** tab page enables you to configure QOS and MOS monitoring threshold values for the specific Session Director (SD) of your choice. After you specify threshold values specific to an SD, the NNM iSPI for IP Telephony lists these threshold values in the **Current Configurations** section and uses them for the specific SD, instead of the threshold values specified in the *Thresholds for QOS/MOS Monitoring* section.

To configure Session Director—specific QOS and MOS monitoring threshold values, follow these steps:

1. On the **Thresholds for QOS/MOS Monitoring** tab page, go to **Session Director Specific Thresholds for QOS/MOS Monitoring** pane > **Add Session Director Specific QOS Configuration** section.
2. Under the **Add Session Director Specific QOS Configuration** section, specify the required details in the fields provided. The following table describes the fields in the section:

Field Name	Description
SD IP Address	The management IP address of the Session Director.
Jitter	The jitter threshold (in milliseconds) to be configured for the SD.
PPL	The Percentage Packet Loss (PPL) threshold to be configured for the cluster. For example, to specify a percentage packet loss threshold of 50%, type 50.
Latency	The latency threshold (in milliseconds) to be configured for the SD.
RFactor	The QoS R-Factor (in percentage) to be configured for the SD. This value must be within the range of 0 to 100.
Avg MOS	The average Mean Opinion Source (MOS) value to be configured for the CM. This value must be within the range of 0.0 to 5.0.

   For more information about the QOS and MOS monitoring parameters, see Configuring the QOS and MOS Threshold Values for Call Monitoring.
3. Click **Add/Modify**. This adds the configuration for the SD in the **Current Configurations** section.

To modify Session Director—specific QOS and MOS monitoring threshold values, follow these steps:

1. From the **Current Configurations** section, select the Session Director—specific configuration that you want to modify .
2. Click **Modify**.
3. In the **Add Session Director Specific QOS Configuration** section, make the required changes.

   Note: You cannot modify the **SD IP Address** value.

4. Click **Add/Modify**. The Session Director—specific configuration is updated with the new values.

To delete Session Director—specific QOS and MOS monitoring threshold values, follow these steps:

1. From the **Current Configurations** section, select the Session Director—specific configuration that you want to delete.
2. Click **Delete**. The Session Director—specific threshold values for the SD are deleted.

   Note: After removing the Session Director—specific threshold value configuration, the NNM iSPI for IP Telephony uses the values you provided in the system-wide *Thresholds for QOS/MOS Monitoring* section.

To export configurations to the Global Manager, follow this step:

- Click **Export All Config to Global Manager**. This sends all the available configuration information listed in the **Current Configuration** section, irrespective of the check boxes selected, to the Global Manager.

  Note: If a global manager is not configured, the NNM iSPI for IP Telephony does not populate any data.

Configuring the Call Termination Cause Codes to be Monitored

The **Call Monitoring Configuration** link on the **Acme Configuration** pane enables you to configure the termination cause codes that need to be monitored for a specific call in the Acme IP Telephony network.

Note: If there are a number of unprocessed Session Director Call Details Records (CDRs), configuring the cause codes, before configuring CDR data access, can generate several incidents.

You can specify the following types of call termination cause codes:

- Success Cause Codes: Lists the cause codes for call terminations that occurred without a call failure. For example, 'Temporary failure', 'User busy'.
- Failure Cause Codes: Lists the cause codes for call terminations that occurred due to a call failure. For example, 'No route destination', 'Service Unavailable'.

After you specify the codes that you want to be monitored, the NNM iSPI for IP Telephony generates the *CallTerminationReason* incident only when the call termination occurs due to one of the specified call termination cause codes.

To configure the monitoring of call termination cause codes, follow these steps:

1. On the NNM iSPI for IP Telephony Cisco Configuration console, click **Call Monitoring Configuration**. The NNM iSPI for IP Telephony Acme Call Monitoring Configuration form opens.
2. On the Call Termination Cause Monitoring tab page, from the types of call termination cause codes sections, select the codes that you want to monitor, and then click > (the **Move Items to Selected List** icon). The sections displayed are as follows:
   - **Success Cause Codes**
   - **Failure Cause Codes**

   Note:
   - To select multiple random cause codes, press the **Ctrl** key and select the required codes.
   - To select a series of cause codes, press the **Shift** key and the select the series of cause codes.
   - To move a selected cause code from the monitored cause code list back to the cause code selection list, select the cause code and click < (the **Move Items to Non-selected List** icon).

   Note: The default version of the property file — `AcmeCDRTerminationCauseCodes.properties` — is available in the following directory:
   - `/var/opt/OV/shared/ipt/conf/acme`

   The property file can be used to add new termination cause codes that are not listed in the types of call termination cause codes section. After you add a new termination cause code, make sure to restart the IPT jboss application server to reflect the change.
3. Click **Apply** to complete the configuration.

Configuring Data Access

You can use the NNM iSPI for IP Telephony Data Access Configuration form to configure the following types of data for Acme Session Director:

- Secure Shell (SSH)
- Call Details Record (CDR)
- Historical Data Recording (HDR)

You can also use this form to modify or delete an existing data access point.

Accessing the Acme Session Director with SSH

Configuring SSH access for the Acme Session Director enables the NNM iSPI for IP Telephony to discover the following features and determines the relationship of these features with each other:

- Session Agent Group
- Network Interface
- Steering Pool
- SIP Interfaces
- SIP Port
- Network Interfaces

To configure SSH access for Acme Session Director, follow these steps:

1. On the NNM iSPI for IP Telephony Cisco Configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Acme Data Access Configuration form opens.
2. Click the **SSH Access** tab.
3. On the **SSH Access** tab page, under the **Add/Modify SSH Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
SD IP Address	Indicates the IP address of the Acme Session Director (SD) for which you want to configure the SSH access.

SSH Type	Indicates the type of SSH application to be used to collect the session details. The NNM iSPI for IP Telephony uses the `ACME_ACLI_DEFAULT` application by default.
User Name	Indicates the user name to be used to establish an SSH connection.
Password	Indicates the password to be used for the user name.
SSH Port	Indicates the port number to be used for the SSH connection.
SSH Timeout	Indicates the number of seconds to wait while attempting to execute a command before canceling the attempt.
Host Key	Indicates the SSH host key for the Acme Session Director.

4. Click **Add/Modify** to complete the configuration. The NNM iSPI for IP Telephony lists the added configuration in the **Current Configurations** section.

To modify an existing SSH configuration for Acme Session Director, follow these steps:

1. Select an existing SSH configuration from the **Current Configurations** section.
2. Click **Modify**.
3. In the **Add/modify SSH Configuration** section, make the required changes.

   Note: You cannot modify the **SD IP Address** and the **SSH Port** values.

4. Click **Add/Modify** to complete the configuration. The NNM iSPI for IP Telephony lists the modified configuration in the **Current Configurations** section.

To delete an existing SSH configuration for Acme Session Director, follow these steps:

1. Select an existing SSH configuration from the **Current Configurations** section.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Accessing the CDR Data

Configuring the CDR data access for the Acme Session Director enables the NNM iSPI for IP Telephony to provide the following reports:

- Acme IP Telephony CDR reports

When the NNM iSPI for IP Telephony is configured as a push receiver, you can configure the CDR access only for one of the Sessions Directors of the redundant pair; which means that if you configure CDR access to the active Session Director of the redundant pair, you cannot configure access for the standby Session Director of the pair and vice versa. However, when an FTP server

is configured to pull the CDR files from the Session Director, you must configure the CDR access for both the active and standby Session Directors of the redundant pair.

Prerequisites

To access the CDR data for Acme Session Director when the NNM iSPI for IP Telephony is configured as a Push reciever, you must configure an FTP server on the NNMi management server (where the NNM iSPI for IP Telephony is installed).

To configure the FTP server on a standalone NNMi management server (a server that is not installed in an HA cluster), follow these steps:

1. Set up an FTP server on the NNMi management server.
2. Create a user on the NNMi management server with the read/write access to the following location:

   Windows:`%NnmDataDir%\shared\ipt\acmecdr`

   Linux: `/var/opt/OV/shared/ipt/acmecdr`
3. Set up the home directory for the FTP server.

   For Windows. Configure the `%NnmDataDir%\shared\ipt\acmecdr` directory as the home directory of the FTP server.

   For Linux. Make sure that the `/` (root) directory is configured as the home directory of the FTP server.

To configure the FTP server on the NNMi management server in an HA cluster, follow these steps:

1. Set up an FTP server on each NNMi management server in the HA cluster.
2. Create a user on the NNMi management server with the read/write access to the following location:

   Note: For the NNM iSPI for IP Telephony installed on Windows, the shared drive must be online when you create this new user.

   Windows:`<Shared_Drive>\NNM\dataDir\shared\ipt\acmecdr`

   Linux: `/nnm_mount_point/NNM/dataDir/shared/ipt/acmecdr`

   In this instance, <*Shared_Drive*> is the drive that is shared among the systems in the HA cluster.

   Tip: If required, create the `acmecdr` directory manually.
3. Set up the home directory for the FTP server.

For Windows. Configure the `<Shared_Drive>\NNM\dataDir\shared\ipt\acmecdr` directory as the home directory of the FTP server.

For Linux. Make sure that the / (root) directory is configured as the home directory of the FTP server.

To configure CDR access for Acme Session Director, follow these steps:

1. On the NNM iSPI for IP Telephony Acme Configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Acme Data Access Configuration form opens.
2. Click the **CDR Access** tab.
3. On the **CDR Access** page, under the **Add/Modify Configuration for Accessing CDR from Acme Session Directors** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Acme SD IP Address	Indicates the Management IP address of the Acme Session Director.
Format Specification File	Indicates the fully qualified path of the property file that describes the fields of the STOP record in the CDR file. The default version of the property file—`AcmeStopCDRRecordFormat.properties`—is available in the following folders: ■ *For Windows*: `%NNMDataDir%\shared\ipt\conf\acme` ■ *For Linux*: `/var/opt/OV/shared/ipt/conf/acme` **Note:** The `cdr-output-inclusive` parameter (disabled by default), in the account configuration file of the Session Director, must be enabled to ensure that the empty fields in the local CDR files are filled with zeros (0s). Else, the NNM iSPI for IP Telephony cannot process the Acme CDRs due to the CDR-field mismatch between the fields defined in the default `AcmeStopCDRRecordFormat.properties` file and the fields in the CDR files of the Session Director. If the `cdr-output-inclusive` parameter cannot be enabled for some reason, make sure that you edit the `AcmeStopCDRRecordFormat.properties` file manually—to include only the non-empty CDR fields from the CDR file of the Session Director in your environment.

CDR Files Download Path	Indicates the path of the directory to which the CDR files are downloaded. When the NNM iSPI for IP Telephony server is configured as a push receiver, this path is configured on the Session Director so that it can push the CDR files. When an FTP server is configured to pull the CDR files from the Session Director, the files are sent to this path. The CDR Files Download Path creates the following folders for each Session Director: ■ **Working**: Contains the CDR files that are in process. ■ **Rejected**: Contains the files that fail parsing. A new incident is generated for the first CDR file that fails parsing and is moved to this folder. Subsequently, an incident is generated for every 10th CDR file that is moved to the folder after it fails parsing. Make sure that you correct the parsing error—such as by editing the respective property file. Else, the IP Telephony Server can run out of disk space as the parsing-failed CDR files continuously get accumulated in the folder. **Note:** The folder for the CDR files to be downloaded for the redundant pair of the Acme Session Director must be created under the following: ■ *For Windows:* `%NNMDataDir%\shared\ipt\acmecdr` ■ *For Linux:* `/var/opt/OV/shared/ipt/acmecdr`

Is IPT SPI Server configured as a push receiver?	Select **True** if the NNM iSPI for IP Telephony server is configured as a Push receiver on the Session Director. **Note:** When the NNM iSPI for IP Telephony is configured as a Push receiver, the raw CDR data of the Acme Session Director is lost. Select **False** if the NNM iSPI for IP Telephony server is not a push receiver. This allows you to configure the FTP credentials to pull the CDR files from the Session Director. To configure the FTP credentials, specify the following details: ▪ **Is it a Secure FTP?**: By default, this field displays **False**. Specify the following credentials: ○ **User Name**: The FTP server user name. ○ **Password**: The password of the FTP server user name. ○ **CDR File Remote Path**: The full path of the directory on the Session Director from where the CDR files are downloaded. ○ **CDR Polling Interval**: The interval (in minutes) at which the NNM iSPI for IP Telephony performs an FTP connect to the Acme Session Director to collect the CDR files. Specify an interval between 2 – 60 minutes. **Note:** The polling interval is a system-wide configuration and is used for all the configured non-push-receiver-based Session Directors for which the NNM iSPI for IP Telephony downloads CDR files using FTP. When the Session Directors are deployed in a pair, the polling occurs only on the active Session Director of the pair; and the NNM iSPI for IP Telephony downloads CDR files—using FTP—only from the active Session Director.

4. Click **Add/Modify** to complete the configuration. The NNM iSPI for IP Telephony lists the added configuration in the **Current Configurations** section.

To modify an existing CDR Access configuration for Acme Session Director, follow these steps:

1. Select an existing CDR Access configuration from the **Current Configurations** section.
2. Click **Modify**.
3. Specify the required values for the configuration in the **Add/Modify Configuration for Accessing CDR from Acme Session Directors** section.

Note: You cannot modify the **Acme SD IP Address** value.

4. Click **Add/Modify** to complete the configuration.

To delete an existing CDR Access configuration for Acme Session Director, follow these steps:

1. Select an existing CDR Access configuration from the **Current Configurations** section.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Note: The default versions of the property files — `AcmeCDRCallSuccessByISDNAndSIPCode.properties` and `AcmeCDRStopRecordParser.properties`— are available in the following directory:

- `/var/opt/OV/shared/ipt/conf/acme`

While the `AcmeCDRCallSuccessByISDNAndSIPCode.properties` file can be used to add the various SIP and ISDN codes to determine if the call can be considered as a successful call in the reports, the `AcmeCDRStopRecordParser.properties` file can be used to add all the possible **Acme-Session-Discposition**, **Acme-Disconnect-Initiator**, **Acme-Disconnect-Cause** and **Acme-SIP-Status** field values from the **Acme CDR Stop Record**. After you edit either of the files, make sure to restart the IPT jboss application server to reflect the change.

Accessing the HDR Data for Acme Session Director

Configuring the HDR access for Acme Session Director enables the NNM iSPI for IP Telephony to provide Acme IP Telephony reports based on the following statistics:

- SIP sessions
- Media set up errors
- ACL (Access Control List) operations
- Transactions
- SIP client operations
- SIP server operations
- Invites

You can configure the HDR access only for one of the sessions directors of the redundant pair; which means that if you configure HDR access to the active session director of the redundant pair, you cannot configure access for the standby session director of the pair and vice versa.

To configure HDR access for Acme Session Director, follow these steps:

1. On the NNM iSPI for IP Telephony Acme Configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Acme Data Access Configuration form opens.

2. Click the **HDR Access** tab.

3. On the **HDR Access** page, under the **Add/Modify Configuration for Accessing HDR from Acme Session Directors**section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Acme SD IP Address	The Management IP address of the Acme Session Director.
HDR Files Download Path	The path of the directory to which the HDR files are downloaded. Each pair of Session Director must have a specific folder to which the HDR files are downloaded. When the NNM iSPI for IP Telephony server is configured as a Push receiver, this path is configured on the Session Director so that it can push the HDR files. The HDR files are pushed from the Session Director to the following directory: ■ *For Windows* – `%NNMDataDir%\\shared\\ipt\\acmehdr\\<New_Directory>` ■ *For Linux* – `/var/opt/OV/shared/ipt/acmehdr/<New_Directory>`

4. Click **Add/Modify** to complete the configuration. The NNM iSPI for IP Telephony lists the added configuration in the **Current Configurations** section.

To modify an existing HDR Access configuration for Acme Session Director, follow these steps:

1. Select an existing HDR Access configuration from the **Current Configurations** section.

2. Click **Modify**.

3. Specify the required values for the configuration in the **Add/Modify Configuration for Accessing HDR from Acme Session Directors** section.

   Note: You cannot modify the **Acme SD IP Address** value.

4. Click **Add/Modify** to complete the configuration.

To delete an existing HDR Access configuration for Acme Session Director, follow these steps:

1. Select an existing HDR Access configuration from the **Current Configurations** section.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Configuring Polling

You can use the NNM iSPI for IP Telephony Acme Polling Configuration form to enable the polling of the Acme IP telephony devices.

To configure the polling of Acme IP telephony devices, follow these steps:

1. On the NNM iSPI for IP Telephony Acme Configuration console, click **Polling Configuration**. The NNM iSPI for IP Telephony Acme Polling Configuration form opens.
2. In the **Session Director Polling** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Configuration for Monitoring the State of Session Directors in HA Pairs or Standalone system	Allows you to configure the continuous polling of the state of Acme Session Director HA pairs or a standalone system. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the Acme Session Director. ▪ Interval: Indicates the interval (in seconds) to poll the Acme Session Director. The default value is 300 seconds.
Configuration for Monitoring the State of Realms of a Session Director	Allows you to configure the continuous polling of the state of the Realms associated with an Acme Session Director. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the Realms. ▪ Interval: Indicates the interval (in seconds) to poll the Realms. The default value is 300 seconds.
Configuration for Monitoring the State of Session Agents of a Session Director	Allows you to configure the continuous polling of the state of the Session Agents associated with an Acme Session Director. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the Session Agents. ▪ Interval: Indicates the interval (in seconds) to poll the Session Agents. The default value is 300 seconds.

3. Click **Apply Changes**.

Configuring Reporting

The **NNM iSPI for IP Telephony Reporting Configuration** form on the **Acme Configuration**console enables you to configure CDR reporting for the Acme Session Directors on the Acme IP Telephony network. However, you have to install and enable the iSPI Performance for Metrics to enable CDR reporting by the NNM iSPI for IP Telephony.

To configure CDR Reporting for Acme Session Directors, follow these steps:

1. On the NNM iSPI for IP Telephony Acme Configuration console, click **Reporting Configuration**. The NNM iSPI for IP Telephony Acme Reporting Configuration form opens.
2. In the **Reports Using CDR Data** section, specify the required details. The following table describes the fields that appear in the section:

Field Name	Description
Enable Reporting	Select the check box to enable the collection and processing of CDRs for reports.
Number of Calls to Write	The number of processed calls to be sent to the Network Performance Server (NPS). The default value is 5000.
Calling and Called Party Numbers in Reports	Select the check box to display the calling party number and the called party numbers in the Call Completion Reports.
Forward to Global Manager	Select the check box if you want the processed call information to be sent from the current management server to the global manager. This option is enabled by default.

3. Click **Apply Changes**.

Avaya IP Telephony

As an administrator, you can configure attributes listed in the table given here for monitoring the Avaya IP telephony infrastructure discovered on the network.

To access the administration console, follow these steps:

1. Log on to the NNMi console as an administrator.
2. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration** > **Avaya Configuration**. The administration console for Avaya IP telephony appears.

The administration console displays configuration options for the following attributes:

Attribute	Description
Call Monitoring	Allows you to configure the call monitoring options of Avaya IP Telephony devices. You can also use this option to view the existing call monitoring configurations.
Data Access	Allows you to configure the NNM iSPI for IP Telephony to access the various categories of management data from the Avaya IP Telephony servers in your deployment environment. You can also use this option to view the existing data access configurations.
Discovery	Allows you to configure the discovery settings for the Avaya primary servers. You can also use this option to view the existing discovery configurations.
IP Phone	Allows you to configure tasks such as specifying the range of IP phones to be excluded from monitoring and enable the custom attributes for the Avaya IP Phones. You can also use this option to view the existing configurations.
Polling	Allows you to configure the polling options of Avaya IP Telephony device states and statistics. You can also use this option to view the existing polling configurations.
Reporting	Allows you to configure the different types of reports for the Avaya IP Telephony network such as Call Details Record (CDR), Phone Media Access Control (MAC), Port Network Load, and Route Pattern Usage. You can also use this option to view the existing reporting configurations.

Configuring Call Monitoring

You can use the NNM iSPI for IP Telephony Avaya Call Monitoring Configuration form to configure the following:

- Monitor the voice QOS metrics and MOS values for calls in the Avaya IP Telephony network
- The termination cause codes that need to be monitored for a specific call in the Avaya IP Telephony network

Configuring the QOS/MOS Threshold Values for Call Monitoring

The **Call Monitoring Configuration** link on the **Avaya Configuration** pane enables you to configure the monitoring of voice QOS metrics and MOS values for calls in the Avaya IP Telephony network. The **Thresholds for QOS/MOS Monitoring** tab on the NNM iSPI for IP Telephony Avaya Call Monitoring Configuration form allows you to specify the threshold values. On violation of set threshold for any of these parameters for any monitored call, the NNM iSPI for IP Telephony generates an incident conveying the resulting values and the set threshold.

To configure the QOS/MOS monitoring threshold values for Avaya IP telephony calls, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Configuration console, click **Call Monitoring Configuration**. The NNM iSPI for IP Telephony Avaya Call Monitoring Configuration form opens.

2. Click the **Thresholds for QOS/MOS Monitoring** tab. The Thresholds for QOS/MOS Monitoring tab page opens.

3. Specify the required details in the fields provided under the **Thresholds for QOS/MOS Monitoring** section of the page. The following table describes the fields that appear under the section:

   Tip: By default, no threshold values are set for these parameters and threshold-based monitoring is disabled. You can enable monitoring and incident generation when you specify the valid threshold values.

QOS/MOS Monitoring Parameter	Description
[1]Jitter	The jitter threshold (in milliseconds) to be configured.
[1]PPL	The Percentage Packet Loss (PPL) threshold to be configured. For example, to specify a percentage packet loss threshold of 50%, type 50.
[1]Latency	The latency (in milliseconds) threshold to be configured.
[1]Avg MOS	The average Mean Opinion Source (MOS) value to be configured. This value must be within the range of 0.0 to 5.0.

   [1]To disable the monitoring, specify **0.0**.

4. Click **Apply Changes**. The NNM iSPI for IP Telephony updates the QOS/MOS monitoring configuration values.

Configuring Communication Manager—specific QOS and MOS Threshold Values

The **Add Communication Manager Specific QOS Configuration** section on the **Thresholds for QOS/MOS Monitoring** tab page enables you to configure QOS and MOS monitoring threshold values for the specific Communication Manager (CM) of your choice. After you specify threshold values specific to a CM, the NNM iSPI for IP Telephony lists these threshold values in the **Current Configurations** section and uses them for the specific CM, instead of the threshold values specified in the *Thresholds for QOS/MOS Monitoring* section.

To configure Communication Manager—specific QOS and MOS monitoring threshold values, follow these steps:

1. On the **Thresholds for QOS/MOS Monitoring** tab page, go to **Communication Manager Specific Thresholds for QOS/MOS Monitoring** pane > **Add Communication Manager Specific QOS Configuration** section.

2. Under the **Add Communication Manager Specific QOS Configuration** section, specify the required details in the fields provided. The following table describes the fields under the section:

Field Name	Description
CM IP Address	The remote IP address of the Communication Manager. Make sure that you specify the same IP address that you provided while configuring the data access for RTCP reception for Avaya IP Telephony. **Note:** If your network supports Network Address Translation (NAT) or Port Address Translation (PAT), specify the external IP address (public address) here.
Jitter	The jitter threshold (in milliseconds) to be configured for the CM.
PPL	The Percentage Packet Loss (PPL) threshold to be configured for the cluster. For example, to specify a percentage packet loss threshold of 50%, type 50.
Latency	The latency threshold (in milliseconds) to be configured for the CM.
Avg MOS	The average Mean Opinion Source (MOS) value to be configured for the CM. This value must be within the range of 0.0 to 5.0.

   For more information about the QOS and MOS monitoring parameters, see Configuring the QOS and MOS Threshold Values for Call Monitoring.

3. Click **Add/Modify**. This adds the configuration for the CM in the **Current Configurations** section.

To modify Communication Manager Specific QOS and MOS monitoring threshold values, follow these steps:

1. From the **Current Configurations** section, select the CM-specific configuration that you want to modify .

2. Click **Modify**.

3. In the **Add Communication Manager Specific QOS Configuration** section, make the required changes.

Note: You cannot modify the **CM IP Address** value.

4. Click **Add/Modify**. The CM-specific configuration is updated with the new values.

To delete Communication Manager Specific QOS and MOS monitoring threshold values, follow these steps:

1. From the **Current Configurations** section, select the CM-specific configuration that you want to delete.
2. Click **Delete**. The CM-specific threshold values for the CM are deleted.

   Note: After removing the CM-specific threshold value configuration, the NNM iSPI for IP Telephony uses the values you provided in the system-wide *Thresholds for QOS/MOS Monitoring* section.

To export configurations to the Global Manager, follow this step:

- Click **Export All Config to Global Manager**. This sends all the available configuration information listed in the **Current Configuration** section, irrespective of the check boxes selected, to the Global Manager.

  Note: If a global manager is not configured, the NNM iSPI for IP Telephony does not populate any data.

Configuring the Call Termination Cause Codes to be Monitored

The **Call Monitoring Configuration** link on the **Avaya Configuration** pane enables you to configure the termination cause codes that need to be monitored for a specific call in the Avaya IP Telephony network.

Note: If there are a number of unprocessed Call Details Records (CDRs) in the Communication Manager, configuring the cause codes, before configuring CDR data access, can generate several incidents.

You can specify the following types of call termination cause codes:

- Success Cause Codes: Lists the cause codes for call terminations that occurred without a call failure. For example, 'Long Duration Call', 'Intraswitch call'.
- Failure Cause Codes: Lists the cause codes for call terminations that occurred due to a call failure. For example, 'Destination Busy', 'Facilities Unavailable'.

After you specify the codes that you want to be monitored, the NNM iSPI for IP Telephony generates the *CallTerminationReason* incident only when the call termination occurs due to one of the specified call termination cause codes.

To configure the monitoring of call termination cause codes, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Configuration console, click **Call Monitoring Configuration**. The NNM iSPI for IP Telephony Avaya Call Monitoring Configuration form opens.
2. Click the **Call Termination Cause Monitoring** tab. The Call Termination Cause Monitoring tab page opens.
3. From the types of call termination cause codes sections, select the codes that you want to monitor, and then click (the **Move Items to Selected List** icon). The sections displayed are as follows:
   - **Success Cause Codes**
   - **Failure Cause Codes**

   Note:
   - To select multiple random cause codes, press the **Ctrl** key and select the required codes.
   - To select a series of cause codes, press the **Shift** key and the select the series of cause codes.
   - To move a selected cause code from the monitored cause code list back to the cause code selection list, select the cause code and click (the **Move Items to Non-selected List** icon).

   Note: The default version of the property file — `avaya-cdr-termination-cause-codes.properties` — is available in the following directory:
   - `%NNMDataDir%\\shared\\ipt\\conf\avaya`

   The property file can be used to add new termination cause codes that are not listed in the types of call termination cause codes section. After you add a new termination cause code, make sure to restart the IPT jboss application server to reflect the change.
4. Click **Apply** to complete the configuration.

Configuring Data Access

You can use the NNM iSPI for IP Telephony Avaya Data Access Configuration form to configure the following types of data for Avaya IP telephony:

- Call Details Record (CDR)
- RTP Control Protocol (RTCP) Reception
- Secure Shell (SSH)

You can also use this form to modify or delete an existing data access point.

Accessing the CDR Data

You can use the NNM iSPI for IP Telephony Data Access Configuration form to configure the CDR data access for Avaya. Configuring the data access for Avaya with CDR enables the NNM iSPI for IP Telephony to provide the following reports:

- Avaya IP Telephony CDR reports
- Avaya IP Telephony Call Types and Termination Reasons reports
- Avaya IP Telephony Trunk Activity reports
- Avaya IP Telephony Media Gateway Call reports

To configure CDR access for Avaya, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Avaya Data Access Configuration form opens.
2. Click the **CDR Access** tab.
3. In the **Add/Modify CDR Access Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
CM IP Address	Indicates the IP address of the Communication Manager server from which the NNM iSPI for IP Telephony can download the CDR files. **Note:** If the primary CM is deployed in duplex redundant pair, this is *not* the virtual or active IP address of the primary CM; this is the IP address of *one of the two physical CM servers* in duplex pair. **Note:** If your network supports Network Address Translation (NAT) or Port Address Translation (PAT), you must specify the external IP address (public address) here.

CDR Format	Indicates the CDR format configured on the Communication Manager server. See the CDR system parameters configuration settings on your Avaya CM to select the correct format.If the CDR Format on the primary Server is Customized, then the CustomizedCDRFormat.properties file can be used the specify the CDR fields and its offsets. **Note:** If the CDR Format on the primary server is `Customized`, you can use the `CustomizedCDRFormat.properties` file to specify the CDR fields and the offsets. For more information about creating a customized CDR file format, see Creating a Customized File.
Circuit ID Modified	Select **True**, if the CDR format chosen on the Communication Manager server is in one of the following formats and if the Communication Manager server is configured to write the modified circuit ID (Trunk Group Member Number) in the CDR records: ■ 59 character ■ Printer ■ TELESEER ■ ISDN-Printer ■ ISDN-TELESEER Check the CDR system parameters configuration settings on your Avaya CM and make sure that you choose the correct settings here.
Date Format	If you select a *Customized* CDR format, then specify the format of the date strings in the CDR records according to the configuration you specified for the date format in the communication manager server configuration. You can select **DDMM** or **MMDD**. DD specifies the date and MM specifies the numeric month. See the CDR system parameters configuration settings on your Avaya CM and select the same date format configured there.

Format Specification File Path	If you select a *Customized* CDR format, then specify the absolute path of the customized CDR format specification file on the NNM iSPI for IP Telephony server. You must prepare this file for each communication manager server before configuring the NNM iSPI for IP Telephony for accessing CDR data from each communication manager server. For more information about creating the customized CDR format specification file, see *Creating Customized CDR Format Specification File*. **Note:** You can use the same customized CDR format specification file for all Avaya CMs in your environment only when you are sure that the CDR formats are same for all Avaya CMs. If you have two or more Avaya CMs with different customized CDR formats, you must create distinct customized CDR format specification files on the NNMi system for each Avaya CM and specify the absolute path to the customized CDR format specification file. See the CDR system parameters configuration settings on all Avaya CMs to verify the CDR formats on the CMs.
Time Zone	Select the time zone of the Avaya CM from the list.

Configured for Survivability	Select **True** if file- based or survivable CDRs are configured on the communication manager for which you are specifying CDR data access configuration. Select **False** if CDR streaming using Reliable Session Protocol (RSP) is configured on the communication manager for which you are specifying CDR data access configuration. See the CDR system parameters configuration settings on your Avaya CM to select the correct choice. **Note:** If Survivability or file based CDR is configured, you must create *one more data access configuration* entry for the IP address of the *other physical Avaya CM server* if the primary CM is a duplex redundant pair of servers. If survivability or file based CDR is not configured and CDR streaming using RSP is configured on the Avaya CM, a single data access configuration using physical IP address of one of the two CM servers in duplex redundant pair would suffice. If you select **True** for this option, you must provide the Secure File Transfer Protocol (SFTP) credentials to be used by NNM iSPI for IP Telephony to download the CDR files programmatically: ■ **SFTP User Name**: Type the SFTP user name to be used for CDR downloads. Check the Avaya CM web based administration to know the correct user name to be used for CDR access. ■ **SFTP Password**: Type the SFTP password for the user name specified. If you select **False** for this option, you must specify the following information to configure CDR data access using RSP: ■ **CDR Port Number**: Type the CDR port number configured on the Avaya CM. Check the CDR IP services configuration on the Avaya CM to determine the CDR port number configured on the CM. You must provide the same port number configured in the Remote Port field of the CDR IP services configurations screen on the CM. ■ **RSP Connectivity Timer**: Type the RSP Connectivity Timer value configured on the Avaya Communication Manager. Check CDR IP services configuration on the Avaya CM to determine the value configured on the CM. You must provide the same value configured in the Connectivity Timer field of the CDR IP Services configurations screen on the CM. ■ **RSP Packet Response Timer**: Type the RSP Packet Response Timer

	value. Check CDR IP services configuration on the Avaya CM to determine the value configured on the CM. You must provide twice the value specified in the Packet Response Timer field in CDR IP Services configurations screen on the CM. ▪ **Is CDR data sent through a CLAN or Processor Ethernet or any other IP node configured on Avaya CM?**: Select **No** if the CDR data is sent directly from the physical Avaya CM. Select **Yes** if the CDR data is sent through a CLAN, Processor, Ethernet, or any other IP node. You must specify the following information if you select **Yes** for this option: ○ **IP Address of remote IP Node**: The IP address of CLAN, Processor, Ethernet, or any other IP node through which the CDR data is sent. Make sure that you provide the IP address of the same node that is configured for this purpose in the Avaya CM. **Tip:** Check CDR IP services configuration and IP node names configurations done on the Avaya CM to determine the IP address of the remote node. The name of this IPv4 node appears as local node on the CDR IP services configuration screen of the CM. You can ascertain the IP address of this IPv4 node by checking the IP node names configurations on the Avaya CM. **Note:** If Survivability or file based CDR is configured, you must create entry for the IP address of the other physical Avaya CM server if the primary CM is a duplex redundant pair of servers.If survivability or file based CDR is not configured and CDR streaming using RSP is configured on the Avaya CM, a single data access configuration using physical IP address of one of the two CM servers in duplex redundant pair would suffice.

4. Click **Add/Modify**. The **Current Configurations** section lists the details of the Communication Managers configured for CDR access.

To modify an Avaya IP Telephony CDR access configuration, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Data Access Configuration form, from the **Current Configurations** section of the **CDR Access** tab, select the configuration that you want to modify.
2. Click **Modify** .
3. In the **Add/Modify CDR Access Configuration** section, make the required changes.

   Note: You cannot modify the **CM IP Address** value.

4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete an Avaya IP Telephony CDR access configuration, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Data Access Configuration page, from the **Current Configurations** section of the **CDR Access** tab, select the configuration that you want to delete.

2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Creating Customized CDR Format Specification Files

If the format for the CDR is specified as customized in the Communication Manager server, you must create a format specification file that provides the CDR parsing information to the NNM iSPI for IP Telephony. This file must include the field names along with the respective offsets in the CDR. The file must display the result for the command `display system-parameters cdr` run on the Communication Manager server as shown in the Sample Customized CDR Format Specification section. The NNM iSPI for IP Telephony includes a sample customized CDR format specification file at the following location:

- `%NNM_DATA_DIR%/shared/ipt/conf/CustomizedCDRFormat.properties` (the `%NNM_DATA_DIR%` represents the NNMi data directory in your NNMi deployment environment)

Sample Customized CDR Format Specification

```
# This file is for specifying customized Avaya CDR records format.

# Line starting with # is ignored.

# Each line contains one field name and its position in CDR file.

# If a fields length is more than one character, the start and end
position

# must be separated using "-" (hyphen).

# IMPORTANT: The positioning starts with 0.

# Examples:

# Dialed Number= 9-16 => Dialed number field starts at position 10 and
ends at 17.

# cond-code = 18 => Condition code is one character available at
position 19 in CDR file.

date=0-5

code-dial=20-23

code-used=25 - 28

calling-num=49-63

# in-TAC is incoming Trunk Access Code
```

```
clg-num/in-tac=100-114

dialed-num=30-47

cond-code=18 #Condition code is one character

duration=

sec-dur=12-16

in-crt-id=78-80

in-trk-code=65-68

out-crt-id=82-84

# Time is HHMM format in 4 digits

time=7-10

auth-code=70-76

acct-code=
```

Configuring RTCP Reception

You can use the NNM iSPI for IP Telephony Data Access Configuration form to configure the RTP Control Protocol (RTCP) reception Configuration for Avaya.

Configuring RTCP reception for Avaya enables the NNM iSPI for IP Telephony to provide the following features:

- Monitoring Voice Quality: Graph Average MOS
- Monitoring Voice Quality: Graph Average Packet Loss
- Monitoring Voice Quality: Graph Jitter
- Monitoring Voice Quality: Graph Latency
- Avaya IP Telephony RTP Session Metrics reports

To configure RTCP access for Avaya, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Avaya Data Access Configuration form opens.
2. Click the **RTCP Reception** tab.
3. In the **Add/Modify RTCP Reception Configuration** section, specify the required details in

the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Enable Reception	Select this check box to enable the NNM iSPI for IP Telephony to receive and process the RTCP packets.
Vendor	Indicates the name of the vendor for the RTCP reception configuration.
Sender Type	Indicates the type of the sender.
IP address on iSPI for IP Telephony system	Indicates the IP address of the NNM iSPI for IP Telephony server where you want to receive RTCP packets from the Avaya end points controlled by the Communication Manager. **Note:** If your network supports Network Address Translation (NAT) or Port Address Translation (PAT), you must specify the external (public) IP address here.
Type of IP address on iSPI for IP Telephony system	Indicates the IP address type for the NNM iSPI for IP Telephony server. **Note:** Only IPv4 addresses are currently supported.
UDP Port on iSPI for IP Telephony system	Indicates the port number on the NNM iSPI for IP Telephony server where you want to receive RTCP packets from the Avaya end points controlled by the Communication Manager.
IP Address of the Communication Manager	Indicates the remote IP address of the Communications Manager. **Note:** If your network supports Network Address Translation (NAT) or Port Address Translation (PAT), you must specify the external IP address (public address) here.
Type of IP address of the Communication Manager	Indicates the remote IP address type of the Communications Manager.
Tenant	Indicates the name of the tenant. You can select the name of the tenant from the drop-down list.
Enable Reporting	Select this check box to configure the NNM iSPI for IP Telephony to start generating the reports for RTP session metrics.

Note:

- You must specify all the details listed to set up an RTCP reception configuration.
- Make sure that you perform the required configuration on the Avaya Communication Manager Server administration tool to specify the listed local IP address and the local port to be the destination of the RTCP packets sent by the end points (IP Phones, H248 Media Gateways, MedPros).configured on the Communication Manager. For more details on the configuration, see the Avaya documentation
- Make sure that the RTCP reception is configured for the end points on the communication manager that is seeded on the same NNM iSPI for IP Telephony server . Do not configure reception of RTCP from communication manager end points unless the communication manager is also seeded on the NNM iSPI for IP Telephony server. For more information on partitioning of RTCP reception across different NNM iSPI for IP Telephony regional manager instances in a GNM environment, see the *NNM iSPI for IP Telephony Deployment Guide*.

4. Click **Add/Modify**. The **Current Configurations** section lists the details of the Communication Managers configured for RTCP Reception.

To modify an Avaya IP Telephony RTCP reception configuration, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Data Access Configuration form, from the **Current Configurations** section of the **RTCP Reception** tab, select the configuration that you want to modify.
2. Click **Modify** .
3. In the **Add/Modify RTCP Reception Configuration** section, select or deselect the Enable Reception and the Enable Reporting check boxes.

   Note: You cannot modify the other details.

4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete an RTCP reception configuration, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Data Access Configuration form, from the **Current Configurations** section of the **RTCP Reception** tab, select the configuration that you want to delete.
2. Click **Delete** . The selected configuration is deleted from the **Current Configurations** section.

Configuring SSH Access

You can use the NNM iSPI for IP Telephony Data Access Configuration form to configure the required Secure Shell (SSH) access details for Avaya. You must configure these details for all the Communication Manager servers in your deployment environment including the standby duplex servers. You can configure the SSH access details by adding the physical IP addresses and the associated credentials for SSH access for all the servers.

Configuring SSH access for Avaya enables the NNM iSPI for IP Telephony to discover and poll the IP addresses for Avaya IP phones.

To configure the SSH access details for Avaya, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Avaya Data Access Configuration form opens.
2. Click the **SSH Access** tab.
3. In the **Add/Modify SSH Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
CM IP Address	Indicates the IP address of the Communication Manager server. **Note:** If your network supports Network Address Translation (NAT) or Port Address Translation (PAT), you must specify the external IP address (public address) here.
SSH Type	Indicates the type of application used to access data on the primary communication manager server. The NNM iSPI for IP Telephony currently supports only System Access Terminal (SAT) application. You cannot edit the value in this box.
User Name	Indicates the SSH user name to log on to the primary Communication Manager server.
Password	Indicates the password for the user name specified.
SSH Port	Indicates the port number on the primary Communication Manager server to which SSH connections can be established from the NNM iSPI for IP Telephony server.
SSH Timeout	Indicates the number of seconds to wait while attempting to execute a command, before canceling the attempt and generating an error.

Host Key	Indicates the host key of the primary Communication Manager server. The NNM iSPI for IP Telephony supports **RSA Level 2** key. An example of RSA Level 2 key is `44 ec ab bc a4 2b a7 47 c5 b0 f4 5a 6f ef 97 d4` (do not specify the bit length of the host key). Contact your administrator of the primary communication manager server to know your RSA Level 2 key.

4. Click **Add/Modify**. The **Current Configurations** section lists all the signaling servers configured for SSH access.

To modify an SSH access configuration for Avaya, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Data Access Configuration form, from the **Current Configurations** section of the **SSH Access** tab, select the configuration that you want to modify.
2. Click **Modify**.
3. In the **Add/Modify SSH Configuration** section, make the required changes.

   Note: You cannot modify the **CM IP Address** and the **SSH Port** values.

4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete an SSH access configuration for Avaya, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Data Access Configuration form, from the **Current Configurations** section of the **SSH Access** tab, select the configuration that you want to delete.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Configuring Discovery Settings for Avaya Primary Servers

You can use the NNM iSPI for IP Telephony Avaya Discovery Configuration form to configure the discovery settings for the Avaya primary servers.

Configuring Discovery Cycle for Avaya Primary Servers

By default, NNMi discovers nodes every 24 hours to identify the changes on your network. This includes the discovery of the IP telephony nodes. The discovery of the Avaya primary servers every 24 hours might result in high system resource utilization, which can impact the call processing.

Keep the Avaya primary server discovery interval at a value that is greater than the default discovery cycle for NNMi. The default recommended discovery interval for the Avaya primary

servers is 90 days (2160 hours) if there are no configuration changes on the Avaya primary servers. If you have made any changes on the network, you can do a configuration poll manually at any time to rediscover the primary servers.

To configure the discovery cycle for Avaya primary servers, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Configuration console, click **Discovery Configuration**. The NNM iSPI for IP Telephony Avaya Discovery Configuration form opens.

2. In the **Primary Servers** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Use NNMi node discovery interval	Clear the check box. This check box is selected by default. If you select this check box, NNMi runs the discovery process for the Avaya primary server according to the discovery interval configured for NNMi. **Note:** You must always keep this check box selected before you do a configuration poll manually. You must clear this check box to type a different discovery interval.
Discovery Interval	Indicates the discovery interval (in hours). The default interval is 2160 hours (90 days). The NNM iSPI for IP Telephony does a periodic discovery of Avaya primary servers based on this interval.

Pause state pollers during discovery	Select this check box to pause the state pollers on a node till the discovery cycle completes for the node. This helps in reducing the system resource usage during discovery. By default, the NNM iSPI for IP Telephony does not pause the state pollers during discovery. Before you pause the state pollers, you must consider the following points: ▪ If you pause the state pollers, the state pollers do not trigger SNMP collection on a node that is being discovered. ▪ The NNM iSPI for IP Telephony does not generate any incidents for some of the state changes on a node during its discovery. ▪ For any state changes for the following entities, the NNM iSPI for IP Telephony does not update the management console with the relevant information: ○ Primary Servers State ○ IP Phone Registration State ○ IPSI Service State ○ MedPros Control Link state & Ethernet Link State ○ Port Network Load ○ Route Pattern Usage ○ Trunk Group Usage ○ DSP Resource Codec ○ Signaling Group Service ○ CM Processor Occupancy

3. Click **Apply Changes**.

Configuring IP Phones

You can use the NNM iSPI for IP Telephony Avaya IP Phone Configuration form to configure the following:

- The range of IP Phone extensions to be excluded from monitoring
- The list of IP Phones to be included for generating incidents at the Registration State Change
- The custom attribute settings for the IP Phones

You can also use this form to modify or delete an existing configuration.

Specifying the Range of Extensions for Avaya Phones to be Excluded from Monitoring

You can specify the range of extensions for phones to be excluded from being monitored for Avaya IP telephony network. After you specify the range of extensions for Avaya, the NNM iSPI for IP Telephony stops monitoring the specified phones. These phones are still discovered in the subsequent discovery cycles, but not shown on the inventory views.

To specify the range of extensions for Avaya phones to be excluded, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Configuration console, click **IP Phone Configuration**. The NNM iSPI for IP Telephony Avaya IP Phone Configuration form opens.
2. In the **Exclusion Configuration** > **Add/Modify IP Phone Exclusion Filter** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
CM IP Address	Indicates the IP address of the Communication Manager for which you want to specify the list of phones to be excluded. **Note:** If your network supports Network Address Translation (NAT) or Port Address Translation (PAT), you must specify the external IP address (public address) here.
Filter	Indicates the IP phones extension range to be excluded. To specify the range of phones to be excluded, follow these points: ▪ Use the hyphen (-) to specify a range of extensions to be excluded. For example, if you want to exclude extensions from 8000 to 8005, you can specify as 8000-8005 in the **Filter** field. ▪ Use asterisk (*), the wildcard character, to specify a set of extensions. For example, if you want to exclude all the extensions that start with 8, you can specify as 8* in the **Filter** field. ▪ Use question mark (?), the wildcard character, to specify extensions that contain specific numerals at specific locations in the extension. For example, if you want to exclude all the extensions that end with 00, you can specify as ???00 in the **Filter** field.

3. Click **Add/Modify**. The configured communication managers for which you want to exclude the list of phones are listed in the **Current Configurations** section.

To modify a specified range of Avaya extensions to be excluded, follow these steps:

1. On the **Exclusion Configuration** section of the NNM iSPI for IP Telephony Avaya IP Phone Configuration form, from the **Current Configurations** section, select the configuration that want to modify.
2. Click **Modify**.
3. In the **Add/Modify IP Phone Exclusion Filter** section, make the required changes.

   Note: You cannot modify the **CM IP Address** value.

4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete a specified range of Avaya extensions to be excluded, follow these steps:

1. On the **Exclusion Configuration** section of the NNM iSPI for IP Telephony Avaya IP Phone Configuration form, from the **Current Configurations** section, select the configuration that want to delete.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Specifying the List of IP Phones for Registration State Change Incident Generation

You can specify a list of IP phones for which the registration state change incident must be generated. You can specify the range based on the Communication Manager that includes the IP phones.

To specify the list of Avaya IP phones for registration state change incident generation, follow these steps:

1. From the **Workspaces** navigation pane, **iSPI for IP Telephony Configuration...**> **Avaya Configuration**. The HP NNM iSPI for IP Telephony Avaya Configuration Console opens.
2. Click **IP Phone Configuration**. The NNM iSPI for IP Telephony Avaya IP Phone Configuration form opens.
3. In the **Inclusion Configuration** > **Add/Modify Filters for IP Phones for which Registration State Change Incidents are to be Generated** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
CM IP Address	Indicates the IP address of the Communications Manager that includes the list of phones for which the registration state change incident must be generated.

Filter	Indicates the extension range to be included. For more information about the extension range, see Specifying the Range of Extensions for Avaya Phones to be Excluded from Monitoring.

4. Click **Add/Modify**. The **Current Configurations** section lists the configured Communication Managers for which you want to generate the incident for registration state changes.

You can select a CM IP address from the list and click **Modify** to modify the existing configuration. However, you cannot modify the **CM IP Address** value.

You can select a CM IP address and click **Delete** to delete the existing configuration.

To modify an existing Inclusion Configuration, follow these steps:

1. On the **Inclusion Configuration** section of the NNM iSPI for IP Telephony Avaya IP Phone Configuration form, from the **Current Configurations** section, select the configuration that want to modify.
2. Click **Modify**.
3. In the **Add/Modify Filters for IP Phones for which Registration State Change Incidents are to be Generated** section, make the required changes.
4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete an existing Inclusion Configuration, follow these steps:

1. On the **Inclusion Configuration** section of the NNM iSPI for IP Telephony Avaya IP Phone Configuration form, from the **Current Configurations** section, select the configuration that want to delete.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Configuring Custom Attribute Settings for the IP Phones

You can use the NNM iSPI for IP Telephony Avaya IP Phone Configuration form to configure the custom attributes settings for the IP Phones. You may enable the custom attributes for the Avaya IP Phones only if these phones are already discovered and stored in the NNMi database. After you enable the custom attributes for Avaya IP Phones, you can see the phone icons for all the discovered Avaya IP Phones in the NNMi topology maps.

To enable the custom attributes for Avaya IP Phones, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration** > **Avaya Configuration**. The HP NNM iSPI for IP Telephony Avaya Configuration Console opens.

2. Click **IP Phone Configuration**. The NNM iSPI for IP Telephony Avaya IP Phone Configuration form opens.
3. In the **Discovery Configuration** section, select the **Enable Phone Custom Attribute Setting** check box.
4. Click **Apply Changes**.

Configuring Polling

You can use the NNM iSPI for IP Telephony Avaya Polling Configuration form to enable polling and set intervals for various pollers that are grouped based on the target to be polled. The pollers are grouped as follows:

- Communication Manager Polling to poll the Avaya Communication Managers
- Media Gateway Polling to poll the Avaya Media Gateways

Configuring the Polling of a Communication Manager

To configure the polling of a Communication Manager, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Configuration console, click **Polling Configuration**. The NNM iSPI for IP Telephony Avaya Polling Configuration form opens.
2. In the **Communication Manager Polling** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Configuration for CLAN and IP Phone Association Monitoring	Allows you to configure the continuous polling of the association between the Avaya IP Phones and the Avaya Control LAN (CLAN) on the network. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the CLAN to find the CLAN and IP Phone association. ▪ Interval: Indicates the interval (in seconds) to poll the CLAN. The default value is 300 seconds.

Configuration for IP Phones Registration State Monitoring	Allows you to configure the continuous polling of the registration state change of the Avaya IP Phones on your network. The available options are as follows: ■ Enable Polling: Select this check box to enable the polling of the Avaya IP Phones. ■ Interval: Indicates the interval (in seconds) to poll the Avaya IP Phones. The default value is 300 seconds.
Configuration for IP Phones IP Address Change Monitoring	Allows you to configure the continuous polling of the IP address change of the Avaya IP Phones on your network. The available options are as follows: ■ Enable Polling: Select this check box to enable the polling of the Avaya IP Phones. ■ Interval: Indicates the interval (in seconds) to poll the Avaya IP Phones. The default value is 900 seconds.
Configuration for Monitoring of Various States of Media Processors	Allows you to configure the continuous polling of the various states of Avaya Media Processors (MedPros, Prowlers) on the network. The available options are as follows: ■ Enable Polling: Select this check box to enable the polling of the media processors. ■ Interval: Indicates the interval (in seconds) to poll the media processors. The default value is 600 seconds.
Configuration for Monitoring of Various States of the IP Server Interfaces (IPSI)	Allows you to configure the continuous polling of the various states of Avaya IP Server Interfaces (IPSI) on the network. The available options are as follows: ■ Enable Polling: Select this check box to enable the polling of the Avaya IP server interface objects. ■ Interval: Indicates the interval (in seconds) to poll the IP server interfaces. The default value is 600 seconds.

Configuration for Monitoring Inter-Region Connection States for IP Network Regions	Allows you to configure the continuous polling of the state of health for the connectivity of the IP Network Region with all the other logically connected IP Network Regions. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the IP Network Regions. ▪ Interval: Indicates the interval (in seconds) to poll the IP Network Regions. The default value is 300 seconds.
Configuration for Monitoring DSP Summaries for IP Network Regions	Allows you to configure the continuous polling of the hourly DSP usage and the related summary of the DSP resources deployed in the Network Region. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the IP Network Regions. ▪ Interval: Indicates the interval (in seconds) to poll the IP Network Regions. The default value is 1800 seconds.
Configuration for Monitoring CODEC Summaries for IP Network Regions	Allows you to configure the continuous polling of the hourly CODEC usage and the related summary of the CODEC resources deployed in the Network Region. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the IP Network Regions. ▪ Interval: Indicates the interval (in seconds) to poll the IP Network Regions. The default value is 1800 seconds.
Configuration for Monitoring the State of Duplex Primary Servers	Allows you to configure the continuous polling of the state (Active/Standby) of the paired Avaya primary servers on the network. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the primary server. ▪ Interval: Indicates the interval (in seconds) to poll the primary server. The default value is 300 seconds.

Configuration for Survivable Server State Monitoring	Allows you to configure the continuous polling of the state (Active/Standby) of the Avaya survivable servers such as Local Survivable Servers (LSP) for every Primary Avaya Communications Manager server on the network. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the survivable server. ▪ Interval: Indicates the interval (in seconds) to poll the survivable server. The default value is 300 seconds.
Configuration for Monitoring Route Pattern Usage Metrics	Allows you to configure the continuous polling of the route pattern usage on the network. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the route pattern usage. ▪ Interval: Indicates the interval (in seconds) to poll the route pattern usage. The default value is 1800 seconds.
Configuration for Monitoring Trunk Group Usage Metrics	Allows you to configure the continuous polling of the trunk group usage metrics on the network. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the trunk group usage. ▪ Interval: Indicates the interval (in seconds) to poll the trunk group usage. The default value is 1800 seconds.
Configuration for Monitoring States of Trunk Group Members and Signaling Groups	Allows you to configure the continuous polling of the state of the trunk group members. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the state of the trunk group members. ▪ Interval: Indicates the interval (in seconds) to poll the state of the trunk group members. The default value is 1800 seconds.
Configuration for Port Network Load Statistics Monitoring	Allows you to configure the continuous polling of the load statistics of the port network. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the load statistics of the port network. ▪ Interval: Indicates the interval (in seconds) to poll the load statistics of the port network. The default value is 1800 seconds.

Configuration for Processor Occupancy Statistics Monitoring	Allows you to configure the continuous polling of the occupancy statistics of the processor. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the occupancy statistics of the processor. ▪ Interval: Indicates the interval (in seconds) to poll the occupancy statistics of the processor. The default value is 1800 seconds.

3. Click **Apply Changes**.

Configuring the Polling of a Media Gateway

To configure the polling of a Media Gateway, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Avaya Configuration**. The NNM iSPI for IP Telephony Avaya Configuration Console opens.
2. Click **Polling Configuration**. The NNM iSPI for IP Telephony Avaya Polling Configuration form opens.
3. In the **Media Gateway Polling** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Configuration for Monitoring the Media Gateway States	Allows you to configure the continuous polling of the state of the media gateways. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the state of the media gateways. ▪ Interval: Indicates the interval (in seconds) to poll the media gateways. The default value is 300 seconds.

Configuration for Monitoring the Media Gateway Module States	Allows you to configure the continuous polling of the state of the media gateway modules. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of state of the media gateway modules. ▪ Interval: Indicates the interval (in seconds) to poll the media gateway modules. The default value is 300 seconds.
Configuration for Monitoring the Media Gateway VoIP Engines States	Allows you to configure the continuous polling of the VoIP engine state of the media gateways. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the VoIP engine state of the media gateways. ▪ Interval: Indicates the interval (in seconds) to poll the VoIP engine of the media gateways. The default value is 300 seconds.
Configuration for Monitoring the Media Gateway DSP Core States	Allows you to configure the continuous polling of the DSP core state of the media gateways. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the state of the DSP core state of the media gateways. ▪ Interval: Indicates the interval (in seconds) to poll the DSP core state of the media gateways. The default value is 300 seconds.

4. Click **Apply Changes**.

Configuring Reporting

The **Reporting Configuration** link on the **Avaya Configuration** console enables you to configure the following types of reports:

- CDR
- Phone Media Access Control (MAC)
- Trunk Activity

- Trunk Group Usage
- Processor Occupancy Summary
- Port Network Load
- IP Network Region DSP/Codec Summary
- Route Pattern Usage

Configuring CDR Reporting

You can use the NNM iSPI for IP Telephony Avaya Reporting Configuration form to configure CDR reporting for Avaya IP Telephony networks. However, you have to install and enable the iSPI Performance for Metrics to enable CDR reporting by the NNM iSPI for IP Telephony.

To configure Avaya CDR reporting, follow these steps:

1. On the NNM iSPI for IP Telephony Avaya Configuration console, click **Reporting Configuration**. The NNM iSPI for IP Telephony Avaya Reporting Configuration form opens.
2. In the **Reports Using CDR Data** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Enable Reporting	Select this check box to enable the Avaya CDR reporting.
Number of Calls to Write	Indicates the number of processed calls to be sent to NPS or the Global Manager in an instance in the field. The default value is 5000.
Calling and Called party Numbers in Reports	Select this check box to display the calling party number and the called party numbers in the Call Details reports.
Forward to Global Manager	Select this check box if you want the processed call information to be sent from the current management server to the global manager. This option is enabled by default.

3. Click **Apply Changes**.

Enabling Phone MAC Reports

You can use the NNM iSPI for IP Telephony Avaya Reporting Configuration form to enable or disable IP Phone MAC comma separated value reports. These reports include information about the IP phones that are added, deleted, or shifted (moved) in the network. After you enable this report, the NNM iSPI for IP Telephony generates this report when a phone is added, removed, or moved on the network.

Note: You must make sure that IP phone discovery is enabled in NNMi for this reporting to work.

To configure IP Phone MAC reporting, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Avaya Configuration**. The NNM iSPI for IP Telephony Avaya Configuration Console opens.
2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Avaya Reporting Configuration form opens.
3. In the **Phone MAC Reports** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Enable Reporting	Select this check box to enable the Avaya IP phone MAC reporting.
Access Switches	Indicates the name of the configuration file that contains the comma-separated list of access switch IP addresses. This field is mandatory if you want the phone MAC reports to include the details regarding the phone shifting in the network. The file is present at the following location: ▪ Windows platforms: `nnmDataDir\shared\ipt\conf` ▪ Non Windows platforms: `/var/opt/OV/shared/ipt/conf`
Forward to Global Manager	Select this check box if you want the phone MAC reporting information to be sent from the current management server to the global manager. This option is enabled by default.

4. Click **Apply Changes**.

You can access these reports from the following location:

- Windows Platforms: `nnmDataDir\shared\ipt\PhoneMacReports\reports`
- Non Windows Platforms: `/var/opt/OV/shared/ipt/PhoneMacReports/reports`

In High Availability environments, you can access these reports from the following location:

- On Windows

  <*Shared_Drive*>`\NNM\dataDir\ipt\PhoneMacReports\reports`

- On UNIX/Linux

*/nnm_mount_point/*NNM/dataDir/ipt/PhoneMacReports/reports

In this instance, <*Shared_Drive*> (Windows) or */nnm_mount_point* (UNIX/Linux) is the

directory location for mounting the NNMi shared disk.

The reports follow the following nomenclature standard: <ipt_server_name>_<vendor name>_ AddPhones_<date>.csv

- ipt_server_name: indicates the name of the NNM iSPI for IP Telephony server if the server is a remote server and the report is generated at the global manager. For local servers, this value gets replaced by the identifier Local.
- vendor name: indicates the name of the vendor, Cisco or Avaya.
- date: indicates the date in mmddyy format when the report was generated.

You can identify if the report is generated for a phone added, moved, or removed by the following identifier in the report name:

- AddPhones: generated for phones added.
- RemovePhones: generated for phones removed from the network.
- MovePhones: generated for phones moved in the network.

The report displays the following details as comma-separated values for a phone addition, removal, or a move.

Report Data	Description
Time stamp	The time at which the change was detected.
Phone extension	The phone extension that was added, removed, or moved.
Phone IP address	The IP address of the phone.
Call Controller IP address	The IP address of the present call controller associated with the phone.
Current switch IP address	The IP address of the present switch.
Current switch interface	The interface name of the present switch.
Previous switch IP address	The IP address of the previous switch associated with the phone.
Previous switch interface	The interface name of the previous switch.

Enabling Trunk Activity Reports

You can use the NNM iSPI for IP Telephony Avaya Reporting Configuration form to enable trunk activity reports.

To configure trunk activity reporting, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Avaya Configuration**. The NNM iSPI for IP Telephony Avaya Configuration Console opens.
2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Avaya Reporting Configuration form.
3. In the **Trunk Activity Report** section, select the **Enable Reporting** check box.
4. Click **Apply Changes**.

Enabling Trunk Group Usage Reports

You can use the NNM iSPI for IP Telephony Avaya Reporting Configuration form to enable trunk group usage reports.

To configure trunk group usage reporting, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration**> **iSPI for IP Telephony Configuration...** > **Avaya Configuration**. The NNM iSPI for IP Telephony Avaya Configuration Console opens.
2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Avaya Reporting Configuration form opens.
3. In the **Trunk Group Usage Report** section, select the **Enable Reporting** check box
4. Click **Apply Changes**.

Enabling Processor Occupancy Summary Reports

You can use the NNM iSPI for IP Telephony Avaya Reporting Configuration form to enable or disable processor occupancy summary reports.

To configure processor occupancy summary reporting, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration**> **iSPI for IP Telephony Configuration...** > **Avaya Configuration**. The NNM iSPI for IP Telephony Avaya Configuration Console opens.

2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Avaya Reporting Configuration form opens.

3. In the **Processor Occupancy Summary Report** section, select the **Enable Reporting** check box

4. Click **Apply Changes**.

Enabling Port Network Load Reports

You can use the NNM iSPI for IP Telephony Avaya Reporting Configuration form to enable or disable port network load reports.

To configure port network load reporting, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Avaya Configuration**. The NNM iSPI for IP Telephony Avaya Configuration Console opens.

2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Avaya Reporting Configuration form opens.

3. In the **Port Network Load Report** section, select the **Enable Reporting** checkbox.

4. Click **Apply Changes**.

Enabling IP Network Region DSP/Codec Summary Report

You can use the NNM iSPI for IP Telephony Avaya Reporting Configuration form to enable or disable IP network region DSP/Codec summary reports.

To configure IP network region DSP/Codec summary reporting, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Avaya Configuration**. The NNM iSPI for IP Telephony Avaya Configuration Console opens.

2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Avaya Reporting Configuration form opens.

3. In the **IP Network Region DSP/Codec Summary Report** section, select the **Enable Reporting** check box.

4. Click **Apply Changes**.

Enabling Route Pattern Usage Report

You can use the NNM iSPI for IP Telephony Avaya Reporting Configuration form to enable or disable route pattern usage reports.

To configure route pattern usage reporting, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Avaya Configuration**. The NNM iSPI for IP Telephony Avaya Configuration Console opens.
2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Avaya Reporting Configuration form opens..
3. In the **Route Pattern Usage Reporting** section, select the **Enable Reporting** check box..
4. Click **Apply Changes**.

Cisco IP Telephony

As an administrator, you can configure the attributes for monitoring the Cisco IP telephony infrastructure discovered on the network.

To access the administration console for Cisco IP telephony, follow these steps:

1. Log on to the NNMi console as an administrator.
2. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration** > **Cisco Configuration**. The administration console for Cisco IP telephony appears.

The console displays configuration options for the following attributes:

Attribute	Description
Call Monitoring	Allows you to configure the call monitoring options of Cisco IP Telephony devices. You can also use this option to view the existing call monitoring configurations.
Data Access	Allows you to configure the NNM iSPI for IP Telephony to access the various categories of management data from the Cisco IP Telephony servers in your deployment environment. You can also use this option to view the existing data access configurations.
Discovery	Allows you to configure the discovery settings for the Cisco H.323 gateways that are configured to a cluster using the H.323 short hostname or the Fully Qualified Domain Name (FQDN). You can also use this option to view the existing discovery configurations.

Attribute	Description
IP Phone	Allows you to configure tasks such as specifying the range of IP phones to be excluded from monitoring and enable the custom attributes for the Cisco IP Phones. You can also use this option to view the existing configurations.
Polling	Allows you to configure the polling options of Cisco IP Telephony device states and statistics. You can also use this option to view the existing polling configurations.
Reporting	Allows you to configure the CDR reporting of Cisco IP Telephony networks. You can also use this option to view the existing reporting configurations.

Configuring the Call Monitoring

You can use the NNM iSPI for IP Telephony Cisco Call Monitoring Configuration form to configure the following:

- Monitor the voice QOS metrics and MOS values for calls in the Cisco IP Telephony network
- The termination cause codes that need to be monitored for a specific call in the Cisco IP Telephony network

Configuring the QOS and MOS Monitoring Threshold Values for Cisco

The **Call Monitoring Configuration** link on the **Cisco Configuration** pane enables you to specify the threshold values for the NNM iSPI for IP Telephony to use while monitoring the voice QOS metrics and MOS values for calls in the Cisco IP Telephony network. On a violation of set threshold for any of these parameters for any monitored call, the NNM iSPI for IP Telephony generates an incident conveying the resulting values and the set threshold.

To configure the QOS and MOS monitoring threshold values for Cisco IP telephony devices, follow these steps:

1. On the NNM iSPI for IP Telephony Cisco Configuration console, click **Call Monitoring Configuration**. The NNM iSPI for IP Telephony Cisco Call Monitoring Configuration form opens.
2. Click the **Thresholds for QOS/MOS Monitoring** tab. The Thresholds for QOS/MOS Monitoring tab page opens.
3. Specify the required details in the fields provided under the **Thresholds for QOS/MOS Monitoring** section of the page.

Tip: By default, no threshold values are set for these parameters and threshold-based monitoring is disabled. The monitoring is enabled when you specify valid threshold values here.

The following table describes the fields that appear under the section:

QOS/MOS Monitoring Parameter	Description
[1]Jitter	Specify the jitter threshold to be configured in milliseconds.
[1]PPL	Specify the Percentage Packet Loss (PPL) threshold to be configured. For example, to specify a percentage packet loss threshold of 50%, type 50 here.
[1]Latency	Specify the latency threshold to be configured in milliseconds.
[2]Avg MOS	Specify the average Mean Opinion Source (MOS) value to be configured. This value must be within the range of 0.0 to 5.0.
[2]Min MOS	Specify the minimum MOS value to be configured. This value must be within the range of 0.0 to 5.0.

[1]To disable the monitoring, specify **-1**.

[2]To disable the monitoring, specify **0.0**.

4. Click **Apply Changes**. The NNM iSPI for IP Telephony updates the QOS/MOS monitoring configuration values.

Configuring Cluster-specific QOS and MOS Monitoring Threshold Values

The **Add Cluster Specific QOS Configuration** section on the **Thresholds for QOS/MOS Monitoring** tab page enables you to configure QOS and MOS monitoring threshold values for a specific clusters of your choice. After you specify threshold values specific to a cluster, the NNM iSPI for IP Telephony lists these threshold values in the **Current Configuration** section and uses them for the cluster, instead of the threshold values specified in the *Thresholds for QOS/MOS Monitoring* section.

To configure cluster-specific QOS and MOS monitoring threshold values, follow these steps:

1. On the **Thresholds for QOS/MOS Monitoring** tab page, go to **Cluster Specific Thresholds for QOS/MOS Monitoring** pane > **Add Cluster Specific QOS Configuration** section.

2. Under the **Add Cluster Specific QOS Configuration** section, specify the required details in the fields provided. The following table describes the fields under the section:

Field Name	Description
Tenant	Select the name of the tenant from the drop-down list.
Cluster ID	Select the required cluster for which you want to configure the threshold values. **Note:** Press and hold down the **SHIFT** key to select multiple clusters.
Jitter	Specify the jitter threshold (in milliseconds) to be configured for the cluster.
PPL	Specify the Percentage Packet Loss (PPL) threshold to be configured for the cluster. For example, to specify a percentage packet loss threshold of 50%, type 50 here.
Latency	Specify the latency threshold to be configured for the cluster.
Avg MOS	Specify the average Mean Opinion Source (MOS) value to be configured for the cluster. This value must be within the range of 0.0 to 5.0.
Min MOS	Specify the minimum MOS value to be configured for the cluster. This value must be within the range of 0.0 to 5.0.

   For more information about the QOS and MOS monitoring parameters, see Configuring the QOS and MOS Monitoring Threshold Values for Cisco.

3. Click **Add/Modify**. This adds the configuration for the cluster in the **Current Configurations** section.

To modify cluster-specific QOS and MOS monitoring threshold values, follow these steps:

1. From the **Current Configurations** section, select the cluster-specific configuration that you want to modify .
2. Click **Modify**. This displays the current threshold values for the cluster in the **Add Cluster Specific QOS Configuration** section.
3. Specify the new values.
4. Click **Add/Modify**. This updates the cluster-specific configuration with the new values.

To delete cluster-specific QOS and MOS monitoring threshold values, follow these steps:

1. From the **Current Configurations** section, select the cluster-specific configuration that you want to delete.

2. Click **Delete**. This deletes the cluster-specific threshold values for the cluster.

   Note: After removing the cluster-specific threshold value configuration, the NNM iSPI for IP Telephony uses the values you provided in the *Thresholds for QOS/MOS Monitoring* section.

To export configurations to the Global Manager, follow this step:

- Click **Export Config to Global Manager**. This sends all the available configuration information listed in the **Current Configurations** section, irrespective of the check boxes selected, to the Global Manager.

Configuring Call Termination Cause Codes to be Monitored

You can configure the NNM iSPI for IP Telephony to monitor only specific call termination cause codes. You can specify the following types of call termination cause codes:

- Call failure cause codes as defined by the International Telecommunication Union (ITU) Q.850: This listing lists the call termination cause codes if a call failure was the reason for the call termination.
- Non failure cause codes as defined by ITU Q.850: This listing lists the call termination cause codes if the call termination occurred normally without a call failure.
- Cisco-specific cause codes: This listing lists call termination cause codes specific to Cisco.

After you specify the codes that you want to be monitored, the NNM iSPI for IP Telephony generates the *CallTerminationReason* incident only when the call termination occurs due to any of the call termination cause codes that you specified.

To configure monitoring of call termination cause codes, follow these steps:

1. On the NNM iSPI for IP Telephony Cisco Configuration console, click **Call Monitoring Configuration**. The NNM iSPI for IP Telephony Cisco Call Monitoring Configuration form opens.
2. Click the **Call Termination Cause Monitoring** tab.
3. You can select the call termination cause codes that you want to monitor from the following sections and click (Move Items to Selected List) to specify the cause codes that you want the NNM iSPI for IP Telephony to monitor:
   - **Failure Cause Codes (Q.850)**
   - **Non Failure Cause Codes (Q.850)**
   - **Cause Codes (Cisco Specific)**

Note:

- To select multiple random cause codes, you can press the **Ctrl** (Control) key and select the required codes
- To select a series of cause codes, you can press the **Shift** key and the select the series of cause codes.
- To move a selected cause code from the monitored cause code list back to the cause code selection list, select the cause code and click < (Move Items to Non Selected List).

Note: The default version of the property file—`CiscoCDRTerminationCauseCodes.properties`—is available in the following directory:

- `%NNMDataDir%\\shared\\ipt\\conf\cisco`

The property file can be used to add new termination cause codes that are not listed in the types of call termination cause codes section. After you add a new termination cause code, make sure to restart the IPT jboss application server to reflect the change.

4. Click **Apply Changes** to complete the configuration.

Configuring Data Access

You can use the Data Access Configuration form to configure the NNM iSPI for IP Telephony to access the following types of data from the Cisco Unified Communications Manager clusters in your deployment environment:

- AVVID XML Layer (AXL) API exposed data
- Call Details Record (CDR) data
- Secure Shell (SSH) data

You can use the AXL and CDR related forms to add a configuration for a cluster, modify the configuration for an existing cluster, or delete an existing configuration for a cluster. You can use the SSH related form for UCM specific configurations.

Configuring the NNM iSPI for IP Telephony to Access the AXL Data

Configuring the data access for Cisco with AXL enables the NNM iSPI for IP Telephony to provide the following features:

- Discover whether or not theUCM node is a Publisher.
  If the role of the UCM is that of a Publisher, the NNM iSPI for IP Telephony discovers and monitors the device pools and the devices associated with each device pool.
- Discover the Publisher UCM for which the `CallManager` service is deactivated or stopped.
  If the `CallManager` service for a Publisher UCM is deactivated or stopped, the NNM iSPI for IP Telephony discovers the UCMs, CM groups, and the UCMs associated with each CM group.
- Provide the Registered Device count of the number of registered IP phones for each of the device pools.
- Monitor the count of registered CTI and VM devices for each device pool.
- Discover the device pools associated with IP phones, H.323 gateways, MGCP gateways, IC trunks, and Media Devices.
- Provide the accurate number of the H.323 Gateway Boxes count of the Registered Devices.
- Monitor the Route List and Hunt List configurations.
- Provide the Route List and Route Group usage reports.
- Provide the P.01 GoS Summary for Route Groups report and the P.01 GoS Summary for Route Lists report.
- Discover the Cisco SRST routers.
- Discover the device pool associated with an SRST router.
- Discover the Locations of a Cisco Unified Communications Manager cluster.
- Map the Call Manager ID from CDR records to the actual CM IP Address or hostname while processing the CDR records.
- Provide the Cisco IP Telephony CDR reports.
  If you do not configure the data access for Cisco with AXL, the Cisco IP Telephony CDR reports show 'NO DATA' for the Call Manager Name and Call Manager IP Address fields.

To configure the AXL data access for Cisco, follow these steps:

1. On the HP NNM iSPI for IP Telephony Cisco configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Cisco Data Access Configuration form opens.
2. Click the **AXL Access** tab.
3. In the **Add/Modify AXL Access Configuration for a Cluster** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Tenant	Select the name of the tenant from the drop-down list.
Cluster ID	Indicates the cluster identifier. You can retrieve this information from the administration web page of the Cisco Unified Communications Manager.
CM IP Address	Indicates the management IP address (public address) of the publisher Cisco Unified Communications Manager in this cluster. The NNM iSPI for IP Telephony uses this IP address to obtain the AXL data for this cluster.
AXL User Name	Indicates the AXL user name to be used for invoking the AXL Web Services.
AXL Password	Indicates the port number on the primary Communication Manager server to which SSH connections can be established from the NNM iSPI for IP Telephony server.

4. Click **Add/Modify** to complete the configuration. The **Current Configurations** section lists all the clusters configured for AXL access.

To modify an AXL access configuration for Cisco, follow these steps:

1. On the NNM iSPI for IP Telephony Data Access Configuration form of Cisco Configuration, from the **Current Configurations** section of the **AXL Access** tab, select the configuration that you want to modify.
2. Click **Modify**.
3. In the **Add/Modify AXL Access Configuration for a Cluster** section, make the required changes.

   Note: You cannot modify the name of the tenant and the cluster ID. If you want to modify the name of the tenant and the cluster ID, you must delete the configuration and create a new configuration with the required changes.

4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete an AXL access configuration for Cisco, follow these steps::

1. On the NNM iSPI for IP Telephony Data Access Configuration form of Cisco Configuration, from the **Current Configurations** section of the **AXL Access** tab, select the configuration that you want to delete.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Accessing the CDR Data

You can use the NNM iSPI for IP Telephony Data Access Configuration form to configure the CDR data access for Cisco. The NNM iSPI for IP Telephony enables you to collect the CDR data in one of the following modes:

- CDRonDemand Web Service mode
- Billing server mode

Configuring the data access for Cisco with CDR enables the NNM iSPI for IP Telephony to provide the following reports:

- Cisco IP Telephony CDR reports
- Cisco IP Telephony Gateway Call reports
- Cisco IP Telephony Trunk Calls reports
- Cisco IP Telephony Call Types and Call Termination Reasons reports

Prerequisites

To access the CDR data for Cisco, you must configure an FTP server on the NNMi management server (where the NNM iSPI for IP Telephony is installed).

To configure the FTP server on a standalone NNMi management server (a server that is not installed in an HA cluster), follow these steps:

1. Set up an FTP server on the NNMi management server.
2. Create a user on the NNMi management server with the read/write access to the following location:

   Windows: `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection`

   Linux: `var/opt/OV/shared/ipt/IPTCiscoCDRCollection`
3. Set up the home directory for the FTP server.

   For Windows. Configure the `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection` directory as the home directory of the FTP server.

   For Linux. Make sure that the / (root) directory is configured as the home directory of the FTP server.
4. *Perform this step only if you want to use SFTP for downloading CDR files from the Cisco Unified Communications Manager server through CDRonDemand Web Service.* Establish a trust relationship for Secure File Transfer Protocol (SFTP) from the Cisco Unified

Communications Manager server (CDR Repository Server) to NNM iSPI for IP Telephony server.

To configure the FTP server on the NNMi management server in an HA cluster, follow these steps:

1. Set up an FTP server on each NNMi management server in the HA cluster.
2. Create a user on the NNMi management server with the read/write access to the following location:

   Note: For the NNM iSPI for IP Telephony installed on Windows, the shared drive must be online when you create this new user.

   Windows: `<Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection`

   Linux: `/nnm_mount_point/NNM/dataDir/shared/ipt/IPTCiscoCDRCollection`

   In this instance, <*Shared_Drive*> is the drive that is shared among the systems in the HA cluster.

   Tip: If required, create the `IPTCiscoCDRCollection` directory manually.

3. Set up the home directory for the FTP server.

   For Windows. Configure the `<Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection` directory as the home directory of the FTP server.

   For Linux. Make sure that the / (root) directory is configured as the home directory of the FTP server.

4. Establish a trust relationship for Secure File Transfer Protocol (SFTP) from the Cisco Unified Communications Manager server (CDR Repository Server) to NNM iSPI for IP Telephony server. Perform this step only if you want to use SFTP for downloading CDR files from the Cisco Unified Communications Manager server through CDROnDemand Web Service.

Additional prerequisites to use the billing server mode

You can configure the NNMi management server as a billing server and export the CDR data from the repository server to the NNMi management server. For this purpose, you must perform the following tasks:

1. Create a directory on the NNMi management server to place all the CDR data. You must create this directory under the following directory:

- For a standalone NNMi management server (a server that is not installed in an HA cluster):
  - *For Windows.* `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection`
  - *For Linux.* `/var/opt/OV/shared/ipt/IPTCiscoCDRCollection`
- For an NNMi management server in an HA cluster:
  - *For Windows.* Configure the `<Shared_ Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection`
  - *For Linux.* `/nnm_mount_point/NNM/dataDir/shared/ipt/IPTCiscoCDRCollection`

2. Configure the Cisco Unified Communications Manager to export CDR files into the newly created directory on the NNMi management server. This configuration task is performed in the Cisco Unified Serviceability console by specifying the Billing Application Server parameters.
3. In the list of parameters, specify the FTP user credentials created.
4. For Directory Path, specify the complete path of the newly created directory if NNMi is installed on a Linux server (`/var/opt/OV/shared/ipt/IPTCiscoCDRCollection/`); specify only the name of the newly created directory if NNMi is installed on a Windows server (`/IPTCiscoCDRCollection/`).

You must configure an FTP or SFTP server on the NNMi management server (where you installed the NNM iSPI for IP Telephony).

For a standalone NNMi management server (a server that is not installed in an HA cluster), do the following:

1. Set up an FTP or SFTP server on the NNMi management server.
2. Create a user on the NNMi management server with the read/write access to the following location:

   Windows: `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection`

   Linux: `/var/opt/OV/shared/ipt/IPTCiscoCDRCollection`
3. Set up the home directory for the FTP or SFTP server.

   For Windows. Configure the `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection` directory as the home directory of the FTP or SFTP server.

   For Linux. Make sure that the `/` (root) directory is configured as the home directory of the FTP or SFTP server

For an NNMi management server in an HA cluster, do the following:

1. Set up an FTP or SFTP server on each NNMi management server in the HA cluster.
2. Create a user on the NNMi management server with the read/write access to the following location:

   Note: For the NNM iSPI for IP Telephony installed on Windows, the shared drive must be online when you create this new user.

   Windows: `<Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection`

   Linux: `/nnm_mount_point/NNM/dataDir/shared/ipt/IPTCiscoCDRCollection`

   In this instance, <*Shared_Drive*> is the drive that is shared among the systems in the HA cluster.

   Tip: If required, create the `IPTCiscoCDRCollection` directory manually.

3. Set up the home directory for the FTP or SFTP server.

   For Windows. Configure the `<Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection` directory as the home directory of the FTP or SFTP server.

   For Linux. Make sure that the / (root) directory is configured as the home directory of the FTP or SFTP server.

To configure CDR access for Cisco, follow these steps:

1. On the NNM iSPI for IP Telephony Cisco Configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Cisco Data Access Configuration form opens.
2. Click the **CDR Access** tab.
3. In the **Add/Modify Configuration for Accessing CDR from Cisco Unified Communications Manager Clusters** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Tenant	Indicates the name of the tenant. You can select the name of the tenant from the drop-down list.

Cluster ID	Indicates the cluster identifier. You can retrieve this information from the administration web page of the Cisco Unified Communications Manager.
CDR Polling Interval	Indicates the interval at which the NNM iSPI for IP Telephony polls for new CDR files from the configured FTP path or invokes the CDRonDemand Web Service to collect the CDR files. For best results, set this interval in the range of 2 minutes to 60 minutes.
Is CDR onDemand WS Based Collection?	Indicates if the `CDRonDemand Web Service` is used to collect the CDR files or not. Select **True** if you want the NNM iSPI for IP Telephony to use the `CDRonDemand Web Service` to collect the CDR files. If you select **True**, specify the following details: ■ **Server IP**: The IP address of the Cisco CDR Repository server. If the server uses overlapping private and public IP addresses in a NAT environment, you must specify the public IP address only. ■ **SOAP User Name**: Simple Object Access Protocol (SOAP) user name of the CDRonDemand WebService. ■ **SOAP Password**: Password for the SOAP user name. ■ **Port**: CDR on demand web service port If you select **False**, specify the complete path to the newly created directory in the CDR Files Download Path box. Cisco Unified Communications Manager considers the NNMi management server as a billing server and exports the CDR data to the path specified in the CDR Files Download Path box. **Tip:** In an Application Failover environment,HP recommends that you select the `CDRonDemand Web Service` mode of data transfer. Otherwise, you must configure two different NNMi servers as billing servers in the Cisco Unified Serviceability console.

4. Click **Add/Modify**. The **Current Configurations** section lists the details of the Cisco Unified Communications Manager configured for CDR access.

To configure SFTP or FTP credentials to be used by CDRonDemand Web Service to send the CDR files to the NNM iSPI for IP Telephony, follow these steps:

1. On the NNM iSPI for IP Telephony Cisco Data Access Configuration form, click the **CDR Access** tab.

2. In the **(S)FTP Server Information to be used by iSPI for IP Telephony** section, of the specify the required details in the fields provided on the page. The following table describes the

fields on the page:

Field Name	Description
Is it a Secure FTP (SFTP) ?	Select **True** if you want to provide an SFTP user name and password. Select **False** if you want to provide an FTP user name and password.
User Name	Indicates a valid SFTP or FTP user name with write privileges on the NNM iSPI for IP Telephony server.
Password	Indicates the password for the SFTP or FTP user name.
Use (S)FTP server FQDN instead of IP Address?	Select **True** if you want the CDR Repository servers to use the FQDN of NNM iSPI for IP Telephony to send the CDR files through FTP or SFTP. Select **False** if you want the CDR Repository servers to use the IP address of NNM iSPI for IP Telephony to send the CDR files. **Note:** Select **False** only if the CDR Repository servers in the Cisco Unified Communications Manager clusters are not able to reach the NNM iSPI for IP Telephony, using the FQDN of NNM iSPI for IP Telephony server. If you select **False**, provide the following details: ▪ **Server FQDN**: The fully qualified domain name of NNM iSPI for IP Telephony. ▪ **Server IP Address**: One of the IP addresses of the NNM iSPI for IP Telephony server. Make sure that this IP address is reachable from the CDR repository nodes in the Cisco Unified Communications Manager clusters. ▪ **Application Failover?**: Select **True** if you have Application Failover setup in your environment or else select **False**. If you select **True**, provide the following details: ○ **Second Server FQDN**: FQDN of the second NNM iSPI for IP Telephony server in Application Failover setup. ○ **Second Server IP Address**: One of the IP addresses of the second NNM iSPI for IP Telephony server. Make sure that this IP address is reachable from CDR repository servers in Cisco Unified Communications Manager clusters.

3. Click **Apply Changes**. This procedure restarts the NNM iSPI for IP Telephony task that monitors the QOS/MOS for IP Telephony calls. The **Current Configurations** section lists

the configured cluster details from which the NNM iSPI for IP Telephony accesses the CDR data.

The NNM iSPI for IP Telephony uses the following directory as the (S)FTP home directory for CDR onDemand Web Service for CDR files collection:

Windows: `<Shared_Drive>\NNM\dataDir\shared\ipt\ IPTCiscoCDRCollection`

UNIX/Linux: `/nnm_mount_point/NNM/dataDir/shared/ipt/IPTCiscoCDRCollection`

To modify the configuration for the CDRonDemand Web Service access for a Cisco Unified Communications Manager Cluster follow these steps:

1. On the NNM iSPI for IP Telephony Data Access Configuration form, from the **Current Configurations** section of the **CDR Access** tab, select the configuration that you want to modify.
2. Click **Modify.**
3. In the **Add/Modify Configuration for Accessing CDR from Cisco Unified Communications Manager Clusters** section, make the required changes.

   Note: You cannot modify the name of the tenant and the cluster ID. If you want to modify the name of the tenant and the cluster ID, you must delete the configuration and create a new configuration with the required changes.
4. Click **Add/Modify**. This procedure restarts the NNM iSPI for IP Telephony task that monitors the QOS/MOS for IP Telephony calls. The **Current Configurations** section lists the modified configurations.

To delete the configuration for the CDRonDemand Web Service access for a Cisco Unified Communications Manager Cluster, follow these steps:

1. On the NNM iSPI for IP Telephony Data Access Configuration form, from the **Current Configurations** section of the **CDR Access** tab, select the configuration that you want to delete.
2. Click **Delete**. This procedure restarts the NNM iSPI for IP Telephony task that monitors the QOS/MOS for IP Telephony calls. The selected configuration is deleted from the **Current Configurations** section.

Accessing the Cisco Unified Communications Manager with SSH

You must configure the required Secure Shell (SSH) access details using the Data Access Configuration form of Cisco Configuration provided by the NNM iSPI for IP Telephony. You must configure these details for all the call manager servers in your deployment environment. When a managed call manager is not configured for SSH data access, it is excluded from the aggregate value that is displayed on the Analysis Pane.

Configuring the data access for Cisco with SSH enables the NNM iSPI for IP Telephony to monitor the following features:

- UCM Call Activity
- Gateway Call Activity
- Media Resource Activity
- Locations
- Cisco TFTP Server
- System Health
- Services

To configure SSH access for a Cisco Unified Communications Manager cluster, follow these steps:

Note: You must complete this task as a prerequisite to start monitoring call attempts handled by a cluster or a call manager. This helps in collecting the required details from the call manager using SSH.

1. On the HP NNM iSPI for IP Telephony Cisco configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Cisco Data Access Configuration form opens.
2. Click the **SSH** tab.
3. On the **SSH Access** tab page, under the **Add/Modify SSH Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
CM IP Address	Indicates the IP address of the call manager for which you want to configure SSH access. **Note:** If your network supports Network Address Translation (NAT) or Port Address Translation (PAT), you must specify the external IP address (public address) here.
SSH Type	Indicates the type of SSH application to be used to collect the call details. The NNM iSPI for IP Telephony uses the `CISCO_UCM_UCOS_DEFAULT` application by default.

User Name	Indicates the user name to be used to establish an SSH connection.
Password	Indicates the password to be used for the user name.
SSH Port	Indicates the port number to be used for the SSH connection.
SSH Timeout	Indicates the number of seconds to wait while attempting to execute a command before canceling the attempt.
Host Key	Indicates the SSH host key for the Cisco Unified Communications Manager.

4. Click **Add/Modify** to complete the configuration. The NNM iSPI for IP Telephony lists the added configuration in the **Current Configuration** section.

To modify an existing SSH configuration for Cisco, follow these steps:

1. Select an existing SSH configuration from the **Current Configurations** section.
2. Click **Modify**.
3. In the **Add/modify SSH Configuration** section, make the required changes.

   Note: You cannot modify the **CM IP Address** and the **SSH Port** values.

4. Click **Add/Modify** to complete the configuration. The NNM iSPI for IP Telephony lists the modified configuration in the **Current Configurations** section.

To delete an existing configuration for Cisco, follow these steps:

1. Select an SSH Configuration from the **Current Configurations** section.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Configuring Discovery Settings for Cisco H.323 Gateways

You can use the NNM iSPI for IP Telephony Cisco Discovery Configuration form to configure the discovery settings for the Cisco H.323 gateways that are configured to a cluster using the H.323 short hostname or the FQDN. The configuration settings ensure that a short hostname or an FQDN is mapped to the H.323 Gateway Bind IP Address to avoid duplicate entries of the gateways during discovery. Without this configuration, an H.323 gateway registered to a cluster (using the Device Name as either a short hostname or an FQDN), does not get discovered by the NNM iSPI for IP Telephony.

To configure the discovery settings for Cisco H.323 gateways, follow these steps:

1. On the HP NNM iSPI for IP Telephony Cisco configuration console, click **Discovery Configuration**. The NNM iSPI for IP Telephony Cisco Discovery Configuration form opens.
2. In the **H.323 Gateway Configuration** > **Add/Modify H.323 Gateway Bind IP Address Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Tenant	Select the name of the tenant from the drop-down list.
Device Name	Indicates the short hostname or the FQDN of the H.323 gateway. **Note:** Make sure that the Device Name of the H.323 gateway is the same as the one that you specified while configuring the gateway to a cluster.
IP Address	Indicates the bind IP address of the H.323 gateway.

3. Click **Add/Modify** to complete the configuration. The configuration is displayed in the **Current Configuration** section.

To modify an H.323 discovery configuration setting, follow these steps:

1. On the NNM iSPI for IP Telephony Cisco Discovery Configuration form, from the **Current Configurations** section, select the configuration that you want to modify.
2. Click **Modify**.
3. In the **Add/Modify H.323 Gateway Bind IP Address Configuration** section, make the required changes.
4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete an H.323 discovery configuration setting, follow these steps:

1. On the NNM iSPI for IP Telephony Cisco Discovery Configuration form, from the **Current Configurations** section, select the configuration that you want to delete.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Configuring IP Phones

You can use the NNM iSPI for IP Telephony Cisco IP Phone Configuration form to configure the following:

- The range of IP Phone extensions to be excluded from monitoring
- The list of IP Phones to be included for generating incidents at the Registration State Change
- The custom attribute settings for the IP Phones

You can also use this form to modify or delete an existing configuration.

Specifying the Range of Extensions for Cisco Phones to be Excluded from Monitoring

You can specify the range of extensions for phones to be excluded from being monitored for Cisco IP telephony network. After you specify the range of extensions, the NNM iSPI for IP Telephony stops monitoring the specified phones. These phones are still discovered in the subsequent discovery cycles, but not shown on the inventory views.

To specify the range of extensions for Cisco IP phones to be excluded, follow these steps:

1. On the HP NNM iSPI for IP Telephony Cisco configuration console, click **IP Phone Configuration**. The NNM iSPI for IP Telephony Cisco IP Phone Configuration form opens.
2. In the **Exclusion Configuration** > **Add/Modify IP Phone Exclusion Filter** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Tenant	Select the name of the tenant that contains the list of IP phones that you want to exclude.
Cluster ID	Indicates the ID of the cluster that contains the list of IP phones that you want to exclude.

Filter	Indicates the IP phones extension range to be excluded. To specify the range of phones to be excluded, follow these points: ▪ Use the hyphen (-) to specify a range of extensions to be excluded. For example, if you want to exclude extensions from 8000 to 8005, you can specify as 8000-8005 in the **Filter** field. ▪ Use asterisk (*), the wildcard character, to specify a set of extensions. For example, if you want to exclude all the extensions that start with 8, you can specify as 8* in the **Filter** field. ▪ Use question mark (?), the wildcard character, to specify extensions that contain specific numerals at specific locations in the extension. For example, if you want to exclude all the extensions that end with 00, you can specify as ???00 in the **Filter** field.

3. Click **Add/Modify**. The **Current Configurations** section lists the configurations that you created to exclude the list of phones to be monitored and discovered.

To modify a specified range of Cisco extensions to be excluded, follow these steps:

1. On the **Exclusion Configuration** section of the NNM iSPI for IP Telephony Cisco IP Phone Configuration form, from the **Current Configurations** section, select the configuration that want to modify.
2. Click **Modify**.
3. In the **Add/Modify IP Phone Exclusion Filter** section, make the required changes.

   Note: You cannot modify the **Tenant** and the **Cluster ID** values.

4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete a specified range of Cisco extensions to be excluded, follow these steps:

1. On the **Exclusion Configuration** section of the NNM iSPI for IP Telephony Cisco IP Phone Configuration form, from the **Current Configurations** section, select the configuration that want to modify.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Specifying the List of IP Phones for Registration State Change Incident Generation

You can specify a list of IP phones, based on the cluster that includes the IP phones, for which the registration state change incident must be generated.

To specify the list of Cisco IP phones for registration state change incident generation, follow these steps:

1. From the **Workspaces** navigation pane, select **Configuration**, and the click **iSPI for IP Telephony Configuration** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco Configuration Console opens.

2. Click **IP Phone Configuration**. The NNM iSPI for IP Telephony Cisco IP Phone Configuration form opens.

3. In the **Inclusion Configuration** > **Add/Modify Filters for IP Phones for which Registration State Change Incidents are to be Generated** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Tenant	Select the name of the tenant that contains the IP phones, for which the registration state change incidents are to be generated.
Cluster ID	Indicates the ID of the cluster that includes the list of phones for which the registration state change incident must be generated .
Filter	Indicates the extension range to be included. For more information, see Specifying the Range of Extensions for Cisco Phones to be Excluded from Monitoring.

4. Click **Add/Modify**. The **Current Configurations** section lists the configured clusters for which you want to generate the incident for registration state changes.

You can select a configuration from the list and click **Modify** to modify the configuration. However, you cannot modify the **Tenant** and **Cluster ID** values.

You can select a configuration and click **Delete** to delete the configuration.

Configuring Custom Attributes Settings for Cisco IP Phones

You can use the NNM iSPI for IP Telephony Configuration form to configure the custom attributes settings for the Cisco IP Phones. You may enable the custom attributes for the Cisco IP Phones only if these phones are already discovered and stored in the NNMi database. If you enable the custom attributes for Cisco IP Phones, you can see the phone icons for all the Cisco IP Phones in the NNMi topology maps.

To enable custom attributes for Cisco IP Phones, follow these steps:

1. From the **Workspaces** navigation pane, select **Configuration**, and then click **iSPI for IP Telephony Configuration...** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco configuration console opens.

2. Click **IP Phone Configuration**. The NNM iSPI for IP Telephony Cisco IP Phone Configuration form opens.

3. In the **Discovery Configuration** section, select the **Enable Phone Custom Attribute Setting** check box.

   Note: You must not enable the custom attributes for Cisco IP Phones if these phones are not discovered in NNMi database.

4. Click **Apply Changes**.

Configuring Polling

You can use the NNM iSPI for IP Telephony Cisco Polling Configuration form to enable polling and set intervals for various pollers that are grouped based on the target to be polled. The pollers are grouped as follows:

- Call Manager Specific Polling to poll the Cisco Unified Communications Manager (CUCM)
- Survivable Remote Site Telephony (SRST) Specific Polling to poll the Cisco SRST routers
- Gatekeeper Specific Polling to poll the Cisco gatekeeper devices
- Unity and Unity Connection Specific Polling to poll their license consumption and port utilization
- Voice Gateway Specific Polling to poll the Cisco voice gateways

Configuring Polling that is Specific to Cisco Unified Communications Manager

To configure the polling specific to Cisco Unified Communications Manager, follow these steps:

1. On the HP NNM iSPI for IP Telephony Cisco configuration console, click **Polling Configuration**. The NNM iSPI for IP Telephony Cisco Polling Configuration form opens.
2. In the **Call Manager Specific Polling Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Monitoring IP Phone Registration State Changes and IP Phone to Call Manager Associations	Allows you to configure the continuous polling of the registration state and controller association of IP Phones. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the Cisco IP Phones. ▪ Interval: Indicates the interval (in seconds) to poll the Cisco IP Phones. The default value is 900 seconds. Internally, the NNM iSPI for IP Telephony also runs a light-weight poller to detect changes in the registration states of Cisco IP Phones within 5 minutes of change on the network. However, the interval of this internal poller cannot be configured. Also note that this internal poller collects incremental registration state change data from each cluster rather than information about all the IP Phones in the Cluster.
Call Manager State Monitoring	Allows you to configure the continuous polling of the state of the CUCM servers. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the state of the CUCM servers. ▪ Interval: Indicates the interval (in seconds) to poll the state of the CUCM servers. The default value is 300 seconds.
Registration State & Controller-Association of Voice Gateway Interfaces Monitoring (MGCP Only)	Allows you to configure the continuous polling of the registration state and controller association of voice gateway interfaces. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the registration state and controller association of voice gateway interfaces. ▪ Interval: Indicates the interval (in seconds) to poll the registration state and controller association of voice gateway interfaces. The default value is 300 seconds.
Monitoring Registration State of Gatekeeper Controlled Inter Cluster Trunks	Allows you to configure the continuous polling of the registration states of Cisco gatekeeper-controlled inter-cluster trunks. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the registration states of Cisco gatekeeper-controlled inter-cluster trunks. ▪ Interval: Indicates the interval (in seconds) to poll the registration states of Cisco gatekeeper-controlled inter-cluster trunks. The default value is 300 seconds.

Registration State of Voice Mail Devices Monitoring	Allows you to configure the continuous polling of the state of the discovered voice mail devices. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the state of the discovered voice mail devices. ▪ Interval: Indicates the interval (in seconds) to poll the state of the discovered voice mail devices. The default value is 300 seconds.

3. Click **Apply Changes**.

Configuring Polling that is Specific to Cisco Survivable Remote Site Telephony (SRST) Routers

To configure the polling specific to SRST, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco Configuration Console opens.
2. Click **Polling Configuration**. The NNM iSPI for IP Telephony Cisco Polling Configuration form opens.
3. In the **Survivable Remote Site Telephony (SRST) Specific Polling Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Survivable Remote Site Telephony (SRST) State Monitoring	Allows you to configure the continuous polling of the available Cisco SRST routers on the network. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the Cisco SRST routers. ▪ Interval: Indicates the interval (in seconds) to poll the Cisco SRST routers. The default value is 300 seconds.

4. Click **Apply Changes**.

Configuring Polling that is Specific to Cisco Gatekeepers

To configure the polling specific to gatekeepers, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco Configuration Console opens.

2. Click **Polling Configuration**. The NNM iSPI for IP Telephony Cisco Polling Configuration form opens.

3. In the **Gatekeeper Specific Polling Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Monitoring Gatekeepers' Count of Registered Endpoints	Allows you to configure the continuous polling of the number of endpoints registered with every gatekeeper. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the number of endpoints registered with every gatekeeper. ▪ Interval: Indicates the interval (in seconds) to poll the number of endpoints registered with every gatekeeper. The default value is 300 seconds.

4. Click **Apply Changes**.

Configuring Polling that is Specific to Unity Devices and Unity Connection Servers

To configure the polling specific to unity devices and unity connection servers, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco Configuration Console opens.

2. Click **Polling Configuration**. The NNM iSPI for IP Telephony Cisco Polling Configuration form opens.

3. In the **Unity and Unity Connection Specific Polling Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

Unity and Unity Connection related License Consumption and Port Utilization Monitoring	Allows you to configure the continuous polling of the license points consumed by the Cisco Unity devices and Unity Connection servers along with the polling of the port utilization. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the consumed license points. ▪ Interval: Indicates the interval (in seconds) to poll the consumed license points. The default value is 300 seconds.

4. Click **Apply Changes**.

Configuring Polling that is Specific to Cisco Voice Gateways

To configure the polling specific to voice gateways, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco Configuration Console opens.
2. Click **Polling Configuration**. The NNM iSPI for IP Telephony Cisco Polling Configuration form opens.
3. In the **Voice Gateway Specific Polling Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Gateway Interface Operational State Monitoring	Allows you to configure the continuous polling of the operational states of voice gateway interfaces. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the operational states of voice gateway interfaces. ▪ Interval: Indicates the interval (in seconds) to poll the operational states of voice gateway interfaces. The default value is 300 seconds.

Voice Gateway Channel Usage State Monitoring	Allows you to configure the continuous polling of the usage states of voice gateway channels. The available options are as follows: ▪ Enable Polling: Select this check box to enable the polling of the usage states of voice gateway channels.. ▪ Interval: Indicates the interval (in seconds) to poll the usage states of voice gateway channels. The default value is 300 seconds.
Voice Gateway Channel Usage Monitoring (Wait Time to Declare Idle)	Allows you to configure the time for which the NNM iSPI for IP Telephony waits, before declaring a channel as idle. The available option is as follows: ▪ Interval: Indicates the interval (in seconds) for which the NNM iSPI for IP Telephony must wait before marking the usage state of a channel to **Idle**. For example, for a waiting time specified as 300 seconds and the period of the usage state monitoring for channels as 150 seconds, during the monitoring of usage state for channels, if the NNM iSPI for IP Telephony finds the usage state to be idle, it waits for two subsequent periodic usage state monitoring cycles. If it still finds the usage in idle state, it declares the state as **Idle**. When the usage state is not **Idle**, the waiting period is not applicable and is abandoned. The default interval is 300 seconds.

4. Click **Apply Changes**.

Configure Reporting

You can use the NNM iSPI for IP Telephony Cisco Reporting Configuration form to configure the following types of reports for Cisco:

- CDR
- B-channel Activity
- Phone Media Access Control (MAC)
- Voice Mail

Configuring CDR Reporting

You can use the NNM iSPI for IP Telephony Cisco Reporting Configuration form to configure CDR reporting for Cisco IP Telephony networks. However, you have to install and enable the iSPI Performance for Metrics to enable CDR reporting by the NNM iSPI for IP Telephony.

To configure the Cisco CDR reporting, follow these steps:

1. On the HP NNM iSPI for IP Telephony Cisco configuration console, click **Reporting Configuration**. The NNM iSPI for IP Telephony Cisco Reporting Configuration form opens.

2. In the **Reports Using CDR Data** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Enable Reporting	Select this check box to enable the Cisco CDR reporting.
Number of Calls to Write	Indicates the number of processed calls to be sent to NPS or the Global Manager in an instance in the field. The default value is 5000.
Calling and Called party Numbers in Reports	Select this check box to display the calling party number and the called party numbers in the Call Details reports.
Forward to Global Manager	Select this check box if you want the processed call information to be sent from the current management server to the global manager. This option is enabled by default.

3. Click **Apply Changes**.

Enabling Cisco B-Channel Activity Reports

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable Cisco B-Channel activity reports.

To configure Cisco B-Channel activity reporting, follow these steps:

1. From the **Workspaces** navigation pane, select **Configuration**, and then click **iSPI for IP Telephony Configuration...** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco configuration console opens.
2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Cisco Reporting Configuration form opens.
3. In the **B-Channel Activity Reports** section, select the **Enable Reporting** check box.
4. Click **Apply Changes**.

Enabling Phone MAC Reports

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable IP phone (MAC) comma-separated value reports. These reports include information about the IP phones that are added, deleted, or shifted (moved) in the network. After you enable this report, the NNM iSPI for IP Telephony generates this report when a phone is added, removed, or moved on the network.

Note: You must make sure that IP phone discovery is enabled in NNMi for this reporting to work. Also, this reporting feature does not work in the NAT environment with overlapping IP addresses.

To configure IP Phone MAC reporting, follow these steps:

1. From the **Workspaces** navigation pane, select **Configuration**, and then click **iSPI for IP Telephony Configuration...** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco configuration console opens.
2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Cisco Reporting Configuration form opens.
3. In the **Phone MAC Reports** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
Enable Reporting	Select this check box to enable the Cisco IP phone MAC reporting.
Access Switches	Indicates the name of the configuration file that contains the comma-separated list of access switch IP addresses. This field is mandatory if you want the phone MAC reports to include the details regarding the phone shifting in the network. The file is present at the following location: ■ Windows platforms: `nnmDataDir\shared\ipt\PhoneMacReports\conf` ■ UNIX/Linux platforms: `/var/opt/OV/shared/ipt/PhoneMacReports/conf`
Forward to Global Manager	Select this check box if you want the phone MAC reporting information to be sent from the current management server to the global manager. This option is enabled by default.

4. Click **Apply Changes**.

You can access the phone MAC reports from the following location:

- Windows Platforms: `nnmDataDir\shared\ipt\PhoneMacReports\reports`
- UNIX/Linux Platforms: `/var/opt/OV/shared/ipt/PhoneMacReports/reports`

In High Availability environments, you can access these reports from the following location:

- On Windows

  <*Shared_Drive*>`\NNM\dataDir\ipt\PhoneMacReports\reports`

- On UNIX/Linux

  /nnm_mount_point/`NNM/dataDir/ipt/PhoneMacReports/reports`

In this instance, <*Shared_Drive*> (Windows) or */nnm_mount_point* (UNIX/Linux) is the

directory location for mounting the NNMi shared disk.

The reports follow the following nomenclature standard: `<ipt_server_name>_<vendor name>_AddPhones_<date>.csv`. The file that is currently being updated displays a `csv.lck` extension name in the file name.

- ipt_server_name: indicates the name of the NNM iSPI for IP Telephony server if the server is a remote server and the report is generated at the global manager. For local servers, this value gets replaced by the identifier `Local`.
- vendor name: indicates the name of the vendor, Cisco or Avaya.
- date: indicates the date in mmddyy format when the report was generated.

You can identify if the report is generated for a phone added, moved, or removed by the following identifier in the report name:

- AddPhones: generated for phones added.
- RemovePhones: generated for phones removed from the network.
- MovePhones: generated for phones moved in the network.

The report displays the following details as comma-separated values for a phone addition, removal, or a move.

Report Data	Description
detected timestamp	The time at which the change was detected.
phoneextn	The phone extension that was added, removed, or moved.
phonemacaddr	The MAC address of the IP phone.
phoneipaddr	The IP address of the phone.
cmipaddr	The IP address of the call manager associated with the phone.
clusterid	The ID of the cluster that includes the phone.

Enabling Voice Mail Reports

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable voice mail reports.

To configure voice mail reporting, follow these steps:

1. From the **Workspaces** navigation pane, select **Configuration**, and then click **iSPI for IP Telephony Configuration...** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco configuration console opens.

2. Click **Reporting Configuration**. The NNM iSPI for IP Telephony Cisco Reporting Configuration form opens.

3. In the **Voice Mail Reports** section, select the **Enable Reporting** check box.

4. Click **Apply Changes**.

Microsoft IP Telephony

As an administrator, you can configure attributes listed in the table below for monitoring the Microsoft IP telephony infrastructure discovered on the network.

To access the administration console, follow these steps:

1. Log on to the NNMi console as an administrator.
2. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration** > **Microsoft Configuration**. The administration console for Microsoft IP telephony appears.

The administration console displays configuration options for the following attributes.

Attribute	Description
Call Monitoring	Allows you to configure the call monitoring options of the Microsoft IP Telephony devices. You can also use this option to view the existing call monitoring configurations.
Frontend	Allows you to configure the discovery of a central Lync site using the front end server pool. You can also use this option to view the existing front end server pool communication configurations.
Gateway	Allows you to configure the polling interval for gateway interfaces and channels. You can also configure the interval for performance data collection for the gateways using this page.
Lync End Users	Allows you to configure Lync end user groups. You can configure end user groups, named end users, and end users to be excluded from monitoring on this page.
Periodic Collection	Allows you to configure periodic collection of CDR and QoE metrics. This page also provides options to configure the interval for user discovery and topology discovery.
Proxy Communication	Allows you to configure the MS IPT proxy with the NNM iSPI for IP Telephony.
Site	Allows you to configure NNMi sites. As an administrator, you can map the discovered Lync Server entities (edge servers, gateways, front end servers, registrar pools, and so on) on the network to the site for ease of administration.

Note: Before running topology discovery for discovering Microsoft Lync servers and gateways, you must enable SNMP on Lync servers and gateways. You must also configure the read community string for the Lync servers and gateways. See the *NNMi Online Help* and the *NNM iSPI for IP Telephony Installation Guide* for Windows for more information.

Configuring Call Monitoring

You can use the NNM iSPI for IP Telephony Microsoft Call Monitoring Configuration form to configure the following:

- Configuring Threshold Values for the Monitoring of QoE
- Configuring the Call Termination Cause Codes to be Monitored

Configuring Threshold Values for the Monitoring of QoE

The **Call Monitoring Configuration** link on the **Microsoft Configuration** pane enables you to configure the monitoring of voice QoE metrics for calls in the Microsoft IP Telephony network. The **Thresholds for QoE Monitoring** tab on the NNM iSPI for Microsoft IP Telephony Monitoring Configuration pane allows you to specify the threshold values. On violation of set threshold for any of these parameters for any monitored call, the NNM iSPI for IP Telephony generates an incident conveying the resulting values and the set threshold.

To configure the QoE monitoring threshold values for Microsoft IP telephony calls, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Call Monitoring Configuration**. The NNM iSPI for IP Telephony Microsoft Monitoring Configuration form opens.
2. Click the **Thresholds for QoE Monitoring** tab. The Thresholds for QoE Monitoring tab page opens.
3. Specify the required details in the fields provided under the **Thresholds for QoE Monitoring** section of the page. The following table describes the fields that appear under the section:

   Tip: By default, the threshold values set for these parameters are **-1** or **0**, and they indicate that the threshold-based monitoring is disabled and incidents will not be generated. You can enable monitoring and incident generation when you specify the valid threshold values.

QoE Monitoring Parameter	Description
Audio Jitter Inter Arrival	The average network jitter (audio) from the Real Time Control Protocol (RTCP) statistics during the call.
Audio Packet Loss Rate	The average packet loss rate (audio) during the call.
Audio Round Trip	The round trip time (audio) from the RTCP statistics during the call.
Video Jitter Inter Arrival	The average network jitter (video) from the RTCP statistics.
Video Packet Loss Rate	The average packet loss rate (video) during the call.
Video Round Trip	The round trip time (video) from the RTCP statistics during the call.
Video Frame Loss Rate	The percentage of total video frames that are lost during the call.
Overall Avg Network MOS	The average wideband Network mean opinion score (MOS) for the call. This metric depends on the packet loss, the jitter and the codec that are used for the call. This value must be within the range of 0.0 to 5.0.
Send Listen MOS	The average predicted wideband Listening MOS for the audio sent to the network during the call. This includes the speech and noise levels, and the capture device characteristics. This value must be within the range of 0.0 to 5.0.
Receive Listen MOS	The average predicted wideband Listening MOS for the audio received from the network during the call. This includes the speech and noise levels, codec, network conditions and the capture device characteristics. This value must be within the range of 0.0 to 5.0.

4. Click **Apply**. The NNM iSPI for IP Telephony updates the QoE monitoring configuration values.

Configuring Site-specific Threshold Values for the Monitoring of QoE

The **Add Site Specific QOE Configuration** section on the **Thresholds for QoE Monitoring** tab page enables you to configure QoE monitoring threshold values for the specific sites of your choice.

After you specify threshold values specific to a site, the NNM iSPI for IP Telephony lists these threshold values in the **Current Configuration** section and uses them for the specific site, instead of the threshold values specified in the *Thresholds for QoE Monitoring* section.

To configure site-specific QoE monitoring threshold values, follow these steps:

1. On the **Thresholds for QoE Monitoring** tab page, go to **Site Specific Thresholds for QoE Monitoring** pane > **Add Site Specific QoE Configuration** section.
2. Under the **Add Site Specific QoE Configuration** section, specify the required details in the fields provided. The following table describes the fields under the section:

Field Name	Description
Site Identity	Select the required site for which you want to configure the threshold values. **Note:** Press and hold down the **SHIFT** key to select multiple sites.
Audio Jitter Inter Arrival	The average network jitter (audio) from the Real Time Control Protocol (RTCP) statistics during the call.
Audio Packet Loss Rate	The average packet loss rate (audio) during the call.
Audio Round Trip	The round trip time (audio) from the RTCP statistics during the call.
Video Jitter Inter Arrival	The average network jitter (video) from the RTCP statistics.
Video Packet Loss Rate	The average packet loss rate (video) during the call.
Video Round Trip	The round trip time (video) from the RTCP statistics during the call.

Video Frame Loss Rate	The percentage of total video frames that are lost during the call.
Overall Avg Network MOS	The average wideband Network mean opinion score (MOS) for the call. This metric depends on the packet loss, the jitter and the codec that are used for the call. This value must be within the range of 0.0 to 5.0.
Send Listen MOS	The average predicted wideband Listening MOS for the audio sent to the network during the call. This includes the speech and noise levels, and the capture device characteristics. This value must be within the range of 0.0 to 5.0.
Receive Listen MOS	The average predicted wideband Listening MOS for the audio received from the network during the call. This includes the speech and noise levels, codec, network conditions and the capture device characteristics. This value must be within the range of 0.0 to 5.0.

For more information about the QoE monitoring parameters, see Configuring Threshold Values for the Monitoring of QoE.

3. Click **Add/Modify**. The configuration value for the site is displayed in the **Current Configuration** section.

To modify site-specific QoE monitoring threshold values, follow these steps:

1. From the **Current Configuration** section, select the site-specific configuration that you want to modify .
2. Click **Modify**. The current threshold values for the site is displayed in the **Add Site Specific QoE Configuration** section.
3. Specify the new values.
4. Click **Add/Modify**. The site-specific configuration is updated with the new values.

Note: You can modify only one site-specific threshold value at a time.

To delete site-specific QoE monitoring threshold values, follow these steps:

1. From the **Current Configuration** section, select the site-specific configuration that you want to delete.
2. Click **Delete**. The site-specific threshold values are deleted .

Note: After removing the site-specific threshold value configuration, the NNM iSPI for IP Telephony uses the values you provided in the *Thresholds for QoE Monitoring* section.

To export configurations to the Global Manager, follow this step:

- Click **Export All Config to Global Manager**. This sends all the available configuration information listed in the **Current Configuration** section, irrespective of the check boxes selected, to the Global Manager.

  Note: If a global manager is not configured, the NNM iSPI for IP Telephony does not populate any data.

Configuring the Call Termination Cause Codes to be Monitored

The **Call Monitoring Configuration** link on the **Microsoft Configuration** pane enables you to configure the termination cause codes that need to be monitored for a specific call in the Microsoft IP Telephony network. You can specify the following types of call termination cause codes:

- Success Cause Codes: Lists the cause codes for call terminations that occurred without a call failure. For example, 'Participant session expired', 'Conference Terminated - Organizer Ended Session'
- Expected Failure Cause Codes: Lists the cause codes for call terminations that occurred due to an expected call failure. For example, 'User does not exist', 'User not found'.
- Unexpected Failure Cause Codes: Lists the cause codes for call terminations that occurred due to an unexpected call failure. For example, 'Service Unavailable', 'Cannot route to destination domain'.

After you specify the codes that you want to be monitored, the NNM iSPI for IP Telephony generates the *CallTerminationReason* incident only when the call termination occurs due to one of the specified call termination cause codes.

To configure the monitoring of call termination cause codes, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Call Monitoring Configuration**. The NNM iSPI for IP Telephony Microsoft Monitoring Configuration form opens.
2. Click the **Call Termination Cause Monitoring** tab. The Call Termination Cause Monitoring tab page opens.
3. From the types of call termination cause codes sections, select the codes that you want to monitor, and then click (the **Move Items to Selected List** icon). The sections displayed are as follows:
   - **Success Cause Codes**
   - **Expected Failure Cause Codes**
   - **Unexpected Failure Cause Codes**

Note:

- To select multiple random cause codes, press the **Ctrl** key and select the required codes.
- To select a series of cause codes, press the **Shift** key and the select the series of cause codes.
- To move a selected cause code from the monitored cause code list back to the cause code selection list, select the cause code and click < (the **Move Items to Non-selected List** icon).

Note: The default version of the property file — `uc-cdr-termination-cause-codes.properties` — is available in the following folder:

- `%NNMDataDir%\\shared\\ipt\\conf\lync`

The property file can be used to add new termination cause codes that are not listed in the types of call termination cause codes section. After you add a new termination cause code, make sure to restart the IPT jboss application server to reflect the change.

4. Click **Apply Changes** to complete this configuration.

Configuring Frontend Server Communication

The NNM iSPI for IP Telephony Microsoft Front End Configuration form lists the front end server pools configured to discover the corresponding central Lync sites.

To view the Frontend Communication Configuration tab page, follow this step:

- On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Frontend Configuration**. The NNM iSPI for IP Telephony Microsoft Front End Configuration form opens. The Frontend Communication Configuration tab page displays the list of the front end server pools configured to discover the corresponding central Lync sites. For information about the attributes related to the front end server pools configured by the administrator on the network, see Adding a New Front End Server Communication Configuration.

You can also select one of the configurations, and then click (the **Open** icon) to view the attribute details of the configuration.

Modifying an Existing Front End Server Communication Configuration

To modify an existing front end server communication configuration, follow these steps:

1. On the **Frontend Communication Configuration** tab page, select the front end server communication configuration that you want to modify.

2. Click (the **Edit** icon). The **Add/Update Frontend Communication Configuration** page opens.

3. Make the required changes, and then click (the **Save** icon) to save the modified configuration settings.

Deleting an Existing Front End Server Communication Configuration

To delete an existing front end server communication configuration, follow these steps:

1. On the **Frontend Communication Configuration** tab page, select the front end server communication configuration that you want to delete.

2. Click (the **Delete** icon). The selected front end server communication configuration is deleted. You can click the **Delete All** icon to delete all the existing front end server communication configurations.

Adding a New Front End Server Communication Configuration

The (**New** icon) on the **Frontend Communication Configuration** tab page enables you to add a new communication configuration. When you click the icon, the **Add/Update Frontend Communication Configuration** page opens. You can use the page to add a new communication configuration to seed a central Lync site for discovery in the NNM iSPI for IP Telephony. You can achieve this by adding the details of the front end server pool in the central Lync site.

Prerequisites for Configuring a New Front End Server Pool

To configure a new front end server pool, you must create a special login for the SQL Server database that is configured to work with Monitoring Server store of the Lync environment.

The login must meet the following requirements:

- While creating this login, select the SQL Server authentication (and not the default Windows authentication).
- The password of the login must never expire.
- The `public` server role must be assigned to the login.
- The login must be mapped to the `LcsCDR` and `QoEMetrics` databases. The `LcsCDR` and `QoEMetrics` databases must be members of the `db_datareader`, `public`, and `ReportsReadOnlyRole` roles.
- The SQL user must be granted the `Execute` permission for the `dbo.pIPIntToString` scalar-valued function.

In addition, the SQL Server database for the Monitoring Server store must use mixed mode authentication (SQL Server and Windows Authentication mode).

To add a new front end server communication configuration, follow these steps:

1. On the **Add/Update Frontend Communication Configuration** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field	Description
Pool Name	Indicates the fully qualified domain name for the front end server pool.
User Name	Indicates the name of the user who can access the systems in the front end server pool. The user must have permissions to run PowerShell commands on the front end servers. Specify the user name in the *domain name\user name* format.
User Password	Indicates the password for the user name.
SQL User	Indicates the login of the SQL Server database that is configured to work with the Monitoring Server store of the Lync environment. The login must meet all the requirements listed in Prerequisites for Configuring a New Front End Server Pool section.
SQL Password	Indicates the password for the SQL user.
Tenant Name	Indicates the tenant name to be associated with the configuration. You can select a tenant name from the list of tenants configured and displayed in the drop-down list. See the *NNMi Online Help* for information about tenants, user groups, and security groups.
Proxy Name	Indicates the name of the proxy to be associated with the front end server pool. You can select a proxy from the list of proxies integrated with the NNM iSPI for IP Telephony.
Pool Description	Indicates the description for the communication configuration.

2. Click (the **Save** icon) to save the new front end server communication configuration.

Configuring Gateway

You can use the NNM iSPI for IP Telephony Microsoft Gateway Configuration form to enable polling and set intervals for the polling of the following types of Lync gateway entities discovered on the network:

- Interface
- Channel
- Performance Data Collection

Configuring Gateway Interface State Polling

You can use the **Interface** tab page on the NNM iSPI for IP Telephony Microsoft Gateway Configuration form to enable polling for gateway interface states and specify the polling interval in minutes.

To configure the gateway interface state polling, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Gateway Configuration**. The NNM iSPI for IP Telephony Microsoft Gateway Configuration form opens.
2. Click the **Interface** tab.
3. On the Interface tab page, select the respective tab for which you want to specify the polling configuration. The following table describes the tabs and the fields that appear on them:

Tab	Description
Administrative State	This tab allows you to specify the configuration to poll the change in the administrative state of the gateway interface. The available options are: ▪ **Enable Polling**: Select this option to enable polling of the administrative state of the gateway interface. ▪ **Polling Interval (mins)**: Specify the interval in minutes to repeat the polling of the administrative state of the gateway interface.
Line Alarm	This tab allows you to specify the configuration to poll the changes in the line alarm state of the gateway interface. Line alarm indicates the presence of active alarms generated at the gateway interface for loop back, failure, and so on. This polling configuration helps you to monitor if there are any active alarms and generates the *GatewayInterfaceLineStatusAlarmed* incident if there are any active alarms present during the polling cycle. The available options are: ▪ **Enable Polling**: Select this option to enable polling of the line alarm state of the gateway interface. ▪ **Polling Interval (mins)**: Specify the interval in minutes to repeat the polling of the line alarm state of the gateway interface.

Operational State	This tab allows you to specify the configuration to poll the change in the operational state of the gateway interface. The available options are: ▪ **Enable Polling**: Select this option to enable polling of the operational state of the gateway interface. ▪ **Polling Interval (mins)**: Specify the interval in minutes to repeat the polling of the operational state of the gateway interface.

4. Click (the **Save** icon) to save the configuration changes.

Configuring Gateway Channel State Polling

You can use the **Channel** tab page on the NNM iSPI for IP Telephony Microsoft Gateway Configuration page to enable polling for gateway channel state and specify the polling interval in minutes.

To configure the gateway channel state polling, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Gateway Configuration**. The NNM iSPI for IP Telephony Microsoft Gateway Configuration form opens.
2. Click the **Channel** tab.
3. On the Channel tab page, select the respective tab for which you want to specify the polling configuration. The following table describes the tabs and the fields that appear on them:

Tab	Description
Operational State	This tab allows you to specify the configuration to poll the change in the operational state of the gateway channel. The available options are: ▪ **Enable Polling**: Select this option to enable polling of the operational state of the gateway channel. ▪ **Polling Interval (mins)**: Specify the interval in minutes to repeat the polling of the operational state of the gateway channel.

Usage State	This tab allows you to specify the configuration to poll the change in the usage state of the gateway channel. The available options are: ▪ **Enable Polling**: Select this option to enable polling of the usage state of the gateway channel. ▪ **Polling Interval (mins)**: Specify the interval in minutes to repeat the polling of the usage state of the gateway channel. ▪ **Hold Time (mins)**: Specify the gateway channel hold time in minutes, to generate the channel idle incident (GatewayChannelStatusIdle) in the event of a gateway channel staying in the idle state for the specified hold time. It is recommended to specify the hold time as a multiple of the polling interval specified. For example, if you had specified a polling interval of five minutes, specify the hold time as 10 minutes.

4. Click (the **Save** icon) to save the configuration changes.

Configuring Gateway Performance Data Collection

You can use the **Performance Data Collection**tab page on the NNM iSPI for IP Telephony Microsoft Gateway Configuration page to enable performance data collection for gateway interface states and specify the data collection interval in minutes.

To configure the gateway performance data collection, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Gateway Configuration**. The NNM iSPI for IP Telephony Microsoft Gateway Configuration form opens.
2. Click the **Performance Data Collection** tab.
3. On the Performance Data Collection tab page, select the respective tab for which you want to specify the data collection configuration. The following table describes the tabs and the fields that appear on them:

Tab	Description

Call Statistics	This tab allows you to specify the configuration for performance data collection for the calls handled by the gateway. The available options are: ▪ **Enable Collection**: Select this option to enable the performance data collection for the calls handled by the gateway. ▪ **Forward to Global Manager**: Select this option if you want the gateway performance data to be sent from the current management server to the global manager. This option is enabled by default. ▪ **Collection Interval (mins)**: Specify the interval in minutes to repeat the performance data collection for the gateways discovered on the network.
B-Channel Activity	This tab allows you to specify the configuration for the collection of B-Channel activity data for generating reports based on the B-Channel usage. The available options are: ▪ **Enable Collection**: Select this option to enable B-Channel activity data collection. ▪ **Forward to Global Manager**: Select this option if you want the B-Channel activity data to be sent from the current management server to the global manager. This option is enabled by default. **Note:** The NNM iSPI for IP Telephony uses the polling interval specified for the **Usage State** of the **Channel** tab page of the NNM iSPI for IP Telephony Microsoft Gateway Configuration form to collect the information about the B-Channel activity..

4. Click (the **Save** icon) to save the configuration changes.

Configuring Lync End Users

You can use the NNM iSPI for IP Telephony Microsoft Lync End Users Configuration form to configure the following types of Lync end user groups based on the end user attributes:

- End user groups
- Named end users
- Excluded end users

This type of configuration helps in gathering the CDR details for a required group of users. A user can be included in multiple user groups. In this event, the lowest reporting order number configured for the user in a group is given priority when gathering the CDR details for that user. You can configure the following types of end user groups:

Creating End User Groups

You can use the **End User Groups** tab page on the NNM iSPI for IP Telephony Microsoft End User Configuration form to view the existing end user groups that are configured. You can also use this page to add new and modify the existing end user groups.

To view the End User Groups tab page, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Lync End Users Configuration**. The NNM iSPI for IP Telephony Microsoft End User Configuration form opens.
2. Click the **End User Groups** tab.
3. The End User Groups tab page displays the list of the configured Lync end user groups. The details displayed on the tab page are described in the following table:

Attribute	Description
End User Group	Indicates the name configured for the end user group.
Reporting Order	Indicates the reporting order configured for the end user group.

You can also select one of the configurations, and then click (the **Open** icon) to view the details of the configuration.

Modifying an Existing End User Group Configuration

To modify an existing end user group configuration, follow these steps:

1. On the **End User Group** tab page, select the configuration that you want to modify.
2. Click (the **Edit** icon). The **Add/Update End User Group Configuration** page opens.
3. Make the required changes, and then click (the **Save** icon) to save the modified configuration settings.

Deleting an Existing Front End Server Communication Configuration

To delete an existing front end server communication configuration, follow these steps:

1. On the **End User Group** tab page, select the configuration that you want to delete.
2. Click (the **Delete** icon). The selected end user group configuration is deleted. You can click the **Delete All** icon to delete all the existing configurations.

Adding a New Lync End User Group

The (**New** icon) on the **End User Groups** tab page enables you to add a new end user group. When you click the icon, the **Add/Update End User Group Configuration** page opens. You can

use the page to add a new end user group configuration.

To add a new end user group configuration, follow these steps:

1. On the **Add/Update End User Group Configuration** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field	Description
Group Name	Indicates the name of the end user group.
Description	Indicates a description of the end user group.
Reporting Order	Indicates the reporting order number to be configured for the end user group. The end user group with the lowest order number is given priority.
Filter Editor Section	Enables you to create a filter to map the required end users under the end user group. This section provides the following options: ▪ Attribute ▪ Operator ▪ Value For more information about the **Filter Editor** section, see About the Filter Editor Section. For more information about defining a filter, see Creating a Filter for an End User Group.

2. Click (the **Save** icon) to save the new end user group configuration.

About the Filter Editor Section

The **Filter Editor** section of the **Add/Update End User Group Configuration** page allows you to do the following:

- You can select one of the following end user attributes from the **Attribute** drop-down list for a filter condition:
  - groupName
  - displayName
  - sipaddress
  - lineURI
  - company
  - countryOrRegionDisplayName

- department
- city
- registrarPool
- targetRegistrarPool
- homeServer
- targetHomeServer
- enabledForRichPresence
- audioVideoDisabled
- voicePolicy
- conferencingPolicy
- dialPlan
- locationPolicy
- clientPolicy
- clientVersionPolicy
- archivingPolicy
- pinPolicy
- externalAccessPolicy
- hostedVoiceMail
- hostedVoiceMailPolicy
- hostingProvider

For the description of these attributes, see Lync End User Form.

- You can select one of the following operators from the **Operator** drop-down list:
  - **=**: Indicates that the filter must be applied on the attribute that matches the exact value provided.
  - **!=**: Indicates that the filter must be applied to the attributes that do not match the value provided.

- **like**: Indicates that the filter must be applied to all the attributes that match the specified value. You can specify a group of attributes using the wildcard characters percent (%) to match a string and the question mark (?) to match a character in the value provided.
- **not like**: Indicates that the filter must be applied to all the attributes that do not match the specified value. You can specify a group of attributes using the wildcard characters percent (%) or asterisk (*) to match a string and the question mark (?) to match a character in the value provided.
- **in**: indicates that the filter must be applied to all the attributes matching the list of values specified. You must specify each value in a separate line when typing multiple values.
- **not in**: indicates that the filter must not be applied to all the attributes that do not match the list of values specified. You must specify each value in a separate line when typing multiple values.

- To insert a filter condition (Attribute, Operator, and Value), use the **Insert** option after selecting the relevant **AND** or **OR** condition.
- To replace a filter condition with a newly specified condition, select the filter condition and then click **Replace**.
- To delete a condition, select the filter condition or an AND or an OR condition, and then click **Delete**.

Creating a Filter for an End User Group

This section gives you an example of creating an end user group based on the following attributes:

- All end users where the *company* attribute is configured as *XYZ*
- All end users where the *display name* has the string *Mgmt%* prefixed to the display name.

To create an end user configuration based on the conditions listed, you must define an end user configuration filter using the **Add/Update End User Group Configuration** page.

To define a filter on the **Add/Update End User Group Configuration** page, follow these steps:

1. Click **AND**. This displays the AND condition parenthesis in the **Filter String** section
2. In the **Filter Editor** section, follow these steps:
   a. From the **Attribute** drop-down list, select **company**.
   b. From the **Operator** drop-down list, select **like**.
   c. In the **Value** box, type `XYZ`.
3. Click **Append**. The **Filter String** section displays the following string: `(company like XYZ)`

4. Click **AND**. The **Filter String** section now displays the following string: `(company like XYZ AND ())`

5. In the **Filter Editor** section, follow these steps:
   a. From the **Attribute** drop-down list, select **displayName**.

   b. From the **Operator** drop-down list, select **like**.

   c. In the **Value** box, type `Mgmt%`.

6. Click **Append**. The **Filter String** section now displays the complete string as: `(company like XYZ AND (displayName like Mgmt%))`.

Creating Named End User Groups

You can use the **Named End Users** tab page on the NNM iSPI for IP Telephony Microsoft End User Configuration form to create end user groups based on the named users discovered on the network. Named users help in the easy identification of users in reports.

To create an end user groups based on the named users, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Lync End Users Configuration**. The NNM iSPI for IP Telephony Microsoft End User Configuration form opens.

2. Click the **Named End Users** tab.

3. On the Named End Users tab page, create a filter to map the required named end users under a named end user group. For more information about creating a filter, see Creating a Filter for Named End Users.

4. Click (the **Save** icon) to save the new named end users configuration.

To view the newly added named end user, click (the **Refresh** icon).

Creating a Filter for Named End Users

This section gives you an example of creating an end user group based on the following attributes:

- All end users where the *company* attribute is configured as *XYZ*
- All end users where the *displayName* has the string *_Mktg* suffixed in the display name.

To create an end user configuration based on the conditions listed , you must define a named end user configuration filter using the **Named End Users** tab page.

To define a filter on the **Named End Users** tab page, follow these steps:

1. Click **AND**. This displays the AND condition parenthesis in the **Filter String** section
2. In the **Filter Editor** section, follow these steps:
   a. From the **Attribute** drop-down list, select **company**.
   b. From the **Operator** drop-down list, select **like**.
   c. In the **Value** box, type `XYZ`.
3. Click **Append**. The **Filter String** section displays the following string: `(company like XYZ)`
4. Click **AND**. The **Filter String** section now displays the following string: `(company like XYZ AND ())`
5. In the **Filter Editor** section, follow these steps:
   a. From the **Attribute** drop-down list, select **displayName**.
   b. From the **Operator** drop-down list, select **like**.
   c. In the **Value** box, type `%_Mktg`.
6. Click **Append**. The **Filter String** section now displays the complete string as: `(company like XYZ AND (displayName like %_Mktg))`.

Creating Excluded End User Groups

You can use the **Excluded End Users** tab page on the NNM iSPI for IP Telephony Microsoft End User Configuration form to create end user groups to be excluded from monitoring.

To create an end user groups based on the excluded users, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Lync End Users Configuration**. The NNM iSPI for IP Telephony Microsoft End User Configuration form opens.
2. Click the **Excluded End Users** tab.
3. On the Excluded End Users tab page, create a filter to map the required excluded end users under an excluded end user group. For more information about creating a filter, see Creating a Filter for Excluded End Users.
4. Click (the **Save** icon) to save the excluded end users configuration.

To view the newly added excluded end user, click (the **Refresh** icon).

Creating a Filter for Excluded End Users

This section gives you an example of creating an end user group based on the following attributes:

- All end users where the *department* attribute is configured as *SrMgmt*.
- All end users where the *city* is *Washington*.

To create an excluded end user configuration based on the conditions listed , you must define an excluded end user configuration filter using the **Excluded End Users** tab page.

To define a filter on the **Excluded End Users** tab page, follow these steps:

1. Click **AND**. This displays the AND condition parenthesis in the **Filter String** section
2. In the **Filter Editor** section, follow these steps:
   a. From the **Attribute** drop-down list, select **department**.
   b. From the **Operator** drop-down list, select **=**.
   c. In the **Value** box, type `SrMgmt`.
3. Click **Append**. The **Filter String** section displays the following string: `(department=SrMgmt)`
4. Click **AND**. The **Filter String** section now displays the following string: `(department=SrMgmt AND ())`
5. In the **Filter Editor** section, follow these steps:
   a. From the **Attribute** drop-down list, select **city**.
   b. From the **Operator** drop-down list, select **=**.
   c. In the **Value** box, type `Washington`.
6. Click **Append**. The **Filter String** section now displays the complete string as: `(department=SrMgmt AND (city=Washington))`.

Note: : You can select one of the following end user attributes from the **Attribute** drop-down list for a filter condition:

- displayName
- sipaddress
- company
- countryOrRegionDisplayName
- department
- city

For the description of these attributes, see Lync End User Form.

Configuring Periodic Collection

You can use the NNM iSPI for IP TelephonyMicrosoft Periodic Collection Configuration form to configure the following:

- Call Details Record (CDR) collection
- Quality of Experience (QoE) score collection
- Topology discovery interval
- User discovery interval

Configuring Call Detail Record Collection

The **CDR** tab page on the NNM iSPI for IP Telephony Microsoft Periodic Collection Configuration form allows you to configure the call details record collection on the Microsoft IP telephony network.

To configure the CDR collection, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Periodic Collection Configuration**. The NNM iSPI for IP Telephony Microsoft Periodic Collection Configuration form opens.
2. Click the **CDR** tab.
3. On the CDR tab page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field	Description
Enable Collection	Select this option to enable CDR collection.
Exclude IM	Select this option to exclude CDR collection for Instant Messaging (IM) sessions.
Forward to Global Manager	Select this option to send the processed call information from the current management server to the global manager. This option is enabled by default.
Interval (mins)	Select the interval in minutes for the CDR collection to be repeated on the network. You can select one of the following intervals: ▪ 15 ▪ 30 ▪ 45 ▪ 60

4. Click (the **Save** icon) to save the CDR collection configuration changes.

Configuring Quality of Experience Collection

The **QoE** tab page on the NNM iSPI for IP Telephony Microsoft Periodic Collection Configuration form allows you to configure the QoE score collection on the Microsoft IP telephony network.

To configure the QoE score collection, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Periodic Collection Configuration**. The NNM iSPI for IP Telephony Microsoft Periodic Collection Configuration form opens.
2. Click the **QoE** tab.
3. On the QoE tab page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field	Description
Enable Collection	Select this option to enable QoE score collection.
Forward to Global Manager	Select this option to send the processed QoE score information from the current management server to the global manager. This option is enabled by default.
Interval (mins)	Select the interval in minutes for the QoE score collection to be repeated on the network. You can select one of the following intervals: ▪ 15 ▪ 30 ▪ 45 ▪ 60

4. Click (the **Save** icon) to save the QoE score collection configuration changes.

Configuring Topology Discovery Details

The **Topology Discovery** tab page on the NNM iSPI for IP Telephony Microsoft Periodic Collection Configuration form helps you to enable topology discovery on the network and schedule the interval in hours for the topology discovery to be repeated on the network.

To enable the topology discovery, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Periodic Collection Configuration**. The NNM iSPI for IP Telephony Microsoft Periodic Collection Configuration form opens.

2. Click the **Topology Discovery** tab.

3. On the Topology Discovery tab page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field	Description
Enable Collection	Select this option to enable topology discovery.
Interval (hrs)	Select the interval in hours for topology discovery to be repeated on the network. You can select one of the following intervals: ■ 12 ■ 24 ■ 48 ■ 60

4. Click (the **Save** icon) to save the topology discovery configuration changes.

Configuring User Discovery Details

The **User Discovery** tab page on the NNM iSPI for IP Telephony Microsoft Periodic Collection Configuration form allows you to configure the user discovery details on the Microsoft IP telephony network.

To enable the user discovery, follow these steps:

1. On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Periodic Collection Configuration**. The NNM iSPI for IP Telephony Microsoft Periodic Collection Configuration form opens.

2. Click the **User Discovery** tab.

3. On the User Discovery tab page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field	Description
Enable Collection	Select this option to enable user discovery.

Interval (hrs)	Select the interval in hours for user discovery to be repeated on the network. You can select one of the following intervals: ▪ 12 ▪ 24 ▪ 48 ▪ 60

4. Click (the **Save** icon) to save the user discovery configuration changes.

Configuring MS IPT Proxy with NNM iSPI for IP Telephony

In Microsoft Lync Server environment, **MS IPT Proxy**, a .NET component is responsible for most of the data collection using remote powershell commands. All the requests (such as topology discovery, and CDR collection) from the NNM iSPI for IP Telephony pass through MS IPT Proxy to the Microsoft Lync server. It is necessary that you install MS IPT Proxy before you start using the NNM iSPI for IP Telephony. For more information about installing MS IPT Proxy, see the *NNM iSPI for IP Telephony Installation Guide for Windows*.

You can install one or more proxies in your environment based on your requirements.

The NNM iSPI for IP Telephony supports the following scenarios:

- Install NNM iSPI for IP Telephony on a Linux server and MS IPT Proxy on a Windows server.
- Install NNM iSPI for IP Telephony on a Windows server and MS IPT Proxy on a different Windows server.
- Install NNM iSPI for IP Telephony and MS IPT Proxy on the same Windows server.

After installing the NNM iSPI for IP Telephony and MS IPT Proxy, you must integrate them so that they communicate with each other. If the NNM iSPI for IP Telephony does not communicate with MS IPT Proxy, the NNM iSPI for IP Telephony cannot discover or monitor the Microsoft Lync Server environment.

To view the proxy communication configurations in your environment, follow this step:

- On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Proxy Communication Configuration**. The NNM iSPI for IP Telephony Microsoft Proxy Communication Configuration form opens.

  The Proxy Communication Configuration tab page displays the list of the proxy communication configurations. The attributes related to the proxy communication configured by the administrator on the network are described in the following table:

Attribute	Description
Proxy Name	Indicates the name given to the MS IPT Proxy by the administrator.
Proxy IP Address	Indicates the IP address of the Windows server on which the MS IPT Proxy is installed.
Proxy Port	Indicates the port number on which MS IPT Proxy is installed.
Status	Indicates whether the proxy is connected with NNM iSPI for IP Telephony or not.
Last Collection Status	Indicates the status of last data collection from the front end server pool using the proxy.

For information about adding a new proxy communication configuration, see Adding a New Proxy Communication Configuration.

Modifying an Existing Proxy Communication Configuration

To modify an existing proxy communication configuration, follow these steps:

1. From the **Proxy Communication Configuration** tab page, select the proxy communication configuration that you want to modify.
2. Click (the **Edit** icon). The **Add/Update Proxy Communication Configuration** page opens.
3. Make the required changes, and then click (the **Save** icon) to save the modified configuration settings.

   Note: You can update only the **Proxy IP Address** and the **Proxy Port** values.

Deleting an Existing Proxy Communication Configuration

To delete an existing proxy communication configuration, follow these steps:

1. From the **Proxy Communication Configuration** tab page, select the proxy communication configuration that you want to delete.
2. Click (the **Delete** icon). The selected proxy communication configuration is deleted. You can click the **Delete All** icon to delete all the existing proxy communication configurations.
3. This deletes the selected proxy communication configuration.

Adding a New Proxy Communication Configuration

The (**New**) icon on the **Proxy Communication Configuration** tab page enables you to add a new proxy communication configuration. When you click the icon, the **Add/Update Proxy**

Communication Configuration page opens. You can use the page to add a new proxy communication configuration to integrate proxies with the NNM iSPI for IP Telephony.

To integrate a proxy communication configuration with theNNM iSPI for IP Telephony, follow these steps:

1. On the **Add/Update Proxy Communication Configuration** page, specify the required details in the fields provided. The following table describes the fields on the page:

Field	Description
Proxy Name	Indicates the name of the MS IPT Proxy. You can give any meaningful name to the proxy; however, you cannot edit this field after the configuration is saved.
Proxy IP Address	Indicates the IP address of the Windows server on which MS IPT Proxy is installed.
Proxy Port	Indicates the port number on which MS IPT Proxy is installed.

Note: You can get the IP address and the port number from the `msipt.proxy.properties` file that is present in the server where you installed MS IPT Proxy. Access this file from the following location in that server:

%NnmDataDir%`\shared\ipt\conf`

2. Click (the **Save** icon) to save the new proxy communication configuration.

Configuring Sites

You can use the NNM iSPI for IP Telephony Microsoft Site Configuration form to view the configured sites as well as create new suite configurations to discover the Lync Server entities such as edge servers, gateways, front end servers, and registrar pools on the network. Creating and maintaining sites eases the task of monitoring the discovered Lync Server entities.

To view the Site Configuration tab page, follow this step:

- On the HP NNM iSPI for IP Telephony Microsoft configuration console, click **Site Configuration**. The NNM iSPI for IP Telephony Microsoft Site Configuration form opens. The Site Configuration tab page displays the list of the sites configured to discover the Lync Server entities. For more information about the attributes of the configured sites, see Adding a New Site Configuration.

  You can also select one of the configurations, and then click (the **Open** icon) to view the attribute details of the configuration.

Modifying an Existing Site Confoguration

To modify an existing end user group, follow these steps:

1. On the **Site Configuration** tab page, select the site that you want to modify.
2. Click (the **Edit** icon). The **Add/Update Site Configuration** page opens.
3. Make the required changes, and then click (the **Save** icon) to save the modified configuration settings.

Deleting an Existing Site Configuration

To delete an existing site, follow these steps:

1. On the **Site Configuration** tab page, select the site that you want to delete.
2. Click (the **Delete** icon). The selected site configuration is deleted. You can click the **Delete All** icon to delete all the existing configurations.

Adding a New Site Configuration

The (**New** icon) on the **Site Configuration** tab page enables you to add a new site configuration. When you click the icon, the **Add/Update Site Configuration** page opens. You can use the page to add a new site configuration and map the necessary Lync Server entities to the site.

To add a new site communication configuration, follow these steps:

1. On the **Add/Update Site Configuration** page, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field	Description
Site	Indicates the name of the site.
Description	Indicates a description of the site.
Order	Indicates the order number to be configured for the site. The site with the lowest order number is given priority.

Field	Description
Site Definition Section	Enables you to create filter to map the required Lync Server entities under the site. This section provides the following options: ▪ Attribute ▪ Operator ▪ Value For more information about the **Site Definition** section, see About the Site Definition Section. For more information about defining a filter, see Creating a Filter for Site Configuration.

2. Click (the **Save** icon) to save the new site communication configuration.

About the Site Definition Section

The **Site Definition** section of the **Add/Update Site Configuration** page allows you to do the following:

- You can select one of the following site attributes from the **Attribute** drop-down list for a filter condition:
  - Edge Server
  - Gateway
  - Registrar Pool
  - Frontend Server
- You can select one of the following operators from the **Operator** drop-down list:
  - **=**: Indicates that the filter must be applied on the attribute that matches the exact value provided.
  - **!=**: Indicates that the filter must be applied to the attributes that do not match the value provided.
  - **like**: Indicates that the filter must be applied to all the attributes that match the specified value. You can specify a group of attributes using the wildcard characters percent (%) to match a string and the question mark (?) to match a character in the value provided.
  - **not like**: Indicates that the filter must be applied to all the attributes that do not match the specified value. You can specify a group of attributes using the wildcard characters percent (%) or asterisk (*) to match a string and the question mark (?) to match a character in the value provided.

- To insert a filter condition (Attribute, Operator, and Value), use the **Insert** option after selecting the relevant **AND** or **OR** condition.
- To replace a filter condition with a newly specified condition, select the filter condition and then click **Replace**.
- To delete a condition, select the filter condition or an AND or an OR condition, and then click **Delete**.

Creating a Filter for Site Configuration

This section gives you an example of creating a site configuration that includes the following Lync Server entities:

- All the front end servers that start with the name *ipt* and *msipt*
- Associated with a registrar pool named *Primary Registrar*

To create a site configuration based on the conditions listed , you must define a site configuration filter using the **Add/Update Site Configuration** page.

To define a filter on the **Add/Update Site Configuration** page, follow these steps:

1. Click **AND**. This displays the AND condition parenthesis in the **Site Definition** section.
2. Click **AND**. This displays the AND condition as a nested condition within the AND condition defined in the previous step.
3. Select the nested AND condition.
4. In the **Site Definition** section, follow these steps:
   a. From the **Attribute** drop-down list, select **Frontend Server**.
   b. From the **Operator** drop-down list, select **like**.
   c. In the **Value** box, type `ipt%`.
5. Click **Append**. The **Filter String** section displays the following string: `(Frontend Server like ipt%)`
6. Select the nested AND condition.
7. In the **Site Definition** section, follow these steps:
   a. From the **Attribute** drop-down list, select **Frontend Server**.
   b. From the **Operator** drop-down list, select **like**.
   c. In the **Value** box, type `msipt%`.

8. Click **Append**. This updates the string as follows: `(Frontend Server like ipt% AND Frontend Server like msipt%)`. This filter string defines the first condition for the site configuration — to filter all the frontend servers names that start with *ipt* and *msipt*.

9. Click **AND**. The **Filter String** section now displays the following string: `((Frontend Server like ipt% AND Frontend Server like msipt%) AND ())`

10. In the **Site Definition** section, follow these steps:
    a. From the **Attribute** drop-down list, select **Registrar Pool**.

    b. From the **Operator** drop-down list, select **=**.

    c. In the **Value** box, type `Primary Registrar`.

11. Click **Append**. The **Filter String** section now displays the complete string as: `((Frontend Server like ipt% AND Frontend Server like msipt%) AND (Registrar Pool = Primary Registrar))`.

Validating the Site Definition

The **Validate Site Definition** tab on the **Add/Update Site Configuration** page allows you to test the validity of the filter that you configured for the Lync Server entities discovered on the network. This opens the Validate Site Definition Result window that displays the results of the filter you configured.

Note: Note:

- The Test Site Definition window displays the details in a tabular format with the **Filter** and **Result** columns.
- The status **Pass** indicates that there were matches for the filter criteria among the list of Lync Server entities discovered on the network.
- The status **Fail** indicates that there were no matches for the filter criteria.

Integrating with SiteScope

You can integrate the NNM iSPI for IP Telephony with HP SiteScope to gather performance metrics for the Microsoft unified communication and collaboration applications that include the Lync Server applications and the Exchange Server application on your network. With this integration, you can collect performance metrics and generate reports using the monitors that SiteScope provides for the following applications:

- Microsoft Exchange
- Microsoft Lync Server applications comprising:
  - Audio/Video conferencing server
  - Archiving server

- Director server
- Edge server
- Frontend server
- Mediation server
- Monitoring server
- Registrar server

Integration Considerations

Make sure that you have the completed the following activities to complete this integration:

- Installed and configured SiteScope according to the instructions provided in the SiteScope documentation before attempting this integration.
- Created a data integration connection using the SiteScope console between SiteScope and NNM iSPI for IP Telephony. See the SiteScope documentation to configure the connection between SiteScope and NNMi.
  - You must specify the URL in the following format in the Receiver URL box if you are using an HTTP connection: `http://IPTHostName:10080/nms-spi-uc-sitescope-war/Sample`. `IPTHostName` refers to the system name where you have installed the NNM iSPI for IP Telephony.
  - If you provide an HTTPS link as the Receiver URL for the data integration, make sure that you import the NNMi license file to SiteScope. See the NNMi Deployment Reference Guide for more information.
  - You must specify the URL in the following format in the Receiver URL box if you are using an HTTPS connection:`https://IPTHOSTName:HTTPS PORT NUMBER/nms-spi-uc-sitescope-war/Sample`
- Enable performance monitoring details to be sent for Microsoft unified communication and collaboration applications from SiteScope to the NNM iSPI for IP Telephony as discussed in the following section.

Enabling Performance Monitoring for Microsoft Unified Communication and Collaboration Applications

1. Log on as an administrator to the NNMi console
2. Click **Integration Module Configuration** > **HP SiteScope IP Telephony**. This opens the HP SiteScope IP Telephony tab page.
3. Select **Microsoft UC Applications Performance Monitoring**

4. Select the **Forward to Global Manager** option if you want the information to be sent from the current management server to the global manager. This option is enabled by default.

5. Click (Save) to save the integration configuration.

Nortel IP Telephony

As an administrator, you can configure attributes listed in the table given here for monitoring the Nortel IP telephony infrastructure discovered on the network.

To access the administration console, do as follows:

1. Log on to the NNMi console as an administrator.

2. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration** > **Nortel Configuration**. The administration console for Nortel IP telephony appears.

The administration console displays configuration options for the following attributes:

Attribute	Description
Data Access	Allows you to configure the NNM iSPI for IP Telephony to access the signaling server data from the Nortel IP Telephony servers in your deployment environment. You can also use this option to view the existing data access configurations.
IP Phone	Allows you to configure tasks such as specifying the range of IP phones to be excluded from monitoring for the Nortel IP Phones. You can also use this option to view the existing configurations.
Polling	Allows you to configure the monitoring options of Nortel IP Telephony device states and statistics. You can also use this option to view the existing monitoring configurations.

Configuring Data Access

You can use the NNM iSPI for IP Telephony Data Access Configuration form to configure the signaling server access for Nortel. You can also use this form to delete the data access points.

To configure the Signaling Server SSH access for Nortel, follow these steps:

1. On the NNM iSPI for IP Telephony Nortel Configuration console, click **Data Access Configuration**. The NNM iSPI for IP Telephony Nortel Data Access Configuration form opens.

2. On the Signaling Server SSH Access tab page, under the **Add/Modify Signaling Server SSH Login Access Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
ELAN IP Address	Indicates the Embedded LAN (ELAN) IP address of the signaling server.
TLAN IP Address	Indicates the Telephony LAN (TLAN) IP address of the signaling server.
Auto Accept Host Key	Indicates if the host key must be accepted automatically for the signaling server. Select **True** to enable this feature.
Host Key Algorithm	Indicates the host key algorithm. You can select one of the following algorithms: ▪ **ssh-rsa**: Authentication using the ssh-rss key pair. ▪ **ssh-dss**: Authentication using the ssh-dss key pair.
Host Key HexFingerprint	Indicates the host key fingerprint in hexadecimal format.
User Name	Indicates the user name to log on to the signaling server.
Password	Indicates the password for the user name specified.
PEM File Location	Indicates the complete path (absolute path) to the location where the PEM file used for authentication is stored This field is applicable only if the public key is used for authentication to log on to the signaling server.
Private Key Password	Indicates the password for the PEM file if the file is encrypted.
Call Server User Name	Indicates the user name to log on to the call server of the signaling server.
Call Server Password	Indicates the password for the user name specified.

3. Click **Add/Modify**. The **Current Configurations** section lists all the signaling servers configured for SSH access.

To modify a Signaling Server SSH access configuration for Nortel, follow these steps:

1. On the NNM iSPI for IP Telephony Data Access Configuration form of Nortel Configuration, from the **Current Configurations** section of the **Signaling Server SSH Access** tab, select the configuration that you want to modify.

2. Click **Modify**.

3. In the **Add/Modify Signaling Server SSH Login Access Configuration** section, make the required changes.

   Note: You cannot modify the **ELAN IP Address** and **TLAN IP Address** values.

4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete a Signaling Server SSH access configuration for Nortel, follow these steps:

1. On the NNM iSPI for IP Telephony Data Access Configuration form of Nortel Configuration, from the **Current Configurations** section of the **Signaling Server SSH Access** tab, select the configuration that you want to delete.

2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Configuring IP Phones

You can use the NNM iSPI for IP Telephony Nortel IP Phone Configuration form to configure the following:

- The range of IP Phone extensions to be excluded from monitoring
- The list of IP Phones to be included for generating incidents at the Registration State Change

Specifying the Range of Extensions for Nortel Phones to be Excluded from Monitoring

You can specify the range of extensions for phones to be excluded from being monitored for Nortel IP telephony network. After you specify the range of extensions for Nortel, the NNM iSPI for IP Telephony stops monitoring these phones and does not discover these phones in the subsequent discovery cycles

To specify the range of extensions for Nortel phones to be excluded, follow these steps:

1. On the NNM iSPI for IP Telephony Nortel Configuration console, click **IP Phone Configuration**. The NNM iSPI for IP Telephony Nortel IP Phone Configuration form opens.

2. In the **Exclusion Configuration** > **Add/Modify IP Phone Exclusion Filter** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description

CS IP Address	Indicates the IP address of the Call Server for which you want to specify the list of phones to be excluded.
Filter	Indicates the IP phones extension range to be excluded. To specify the range of phones to be excluded, follow these points: ▪ Use the hyphen (-) to specify a range of extensions to be excluded. For example, if you want to exclude extensions from 8000 to 8005, you can specify as 8000-8005 in the **Filter** field. ▪ Use asterisk (*), the wildcard character, to specify a set of extensions. For example, if you want to exclude all the extensions that start with 8, you can specify as 8* in the **Filter** field. ▪ Use question mark (?), the wildcard character, to specify extensions that contain specific numerals at specific locations in the extension. For example, if you want to exclude all the extensions that end with 00, you can specify as ???00 in the **Filter** field.

3. Click **Add/Modify**. The configured call servers for which you want to exclude the list of phones are listed in the **Current Configurations** section.

To modify a specified range of Nortel extensions to be excluded, follow these steps:

1. On the NNM iSPI for IP Telephony IP Phone Exclusion Configuration form (for **Nortel Configuration**), from the **Current Configurations** section, select the configuration that want to modify.
2. Click **Modify**.
3. In the **Add/Modify IP Phone Exclusion Filter** section, make the required changes.
4. Click **Add/Modify**. The modified configuration is listed in the **Current Configurations** section.

To delete a specified range of Nortel extensions to be excluded, follow these steps:

1. On the NNM iSPI for IP Telephony IP Phone Exclusion Configuration form (for **Nortel Configuration**), from the **Current Configurations** section, select the configuration that want to delete.
2. Click **Delete**. The selected configuration is deleted from the **Current Configurations** section.

Specifying the List of IP Phones for Registration State Change Incident Generation

You can specify a list of IP phones for which the registration state change incident must be generated. You can specify a range of IP phones based on the Call Server that includes the IP phones.

To specify the list of IP phones for registration state change incident generation, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration** > **Nortel Configuration**. The NNM iSPI for IP Telephony configuration form opens.

2. Click **IP Phone Configuration**. The NNM iSPI for IP Telephony Nortel IP Phone Configuration form opens.

3. In the **Inclusion Configuration** > **Add/Modify Filters for IP Phones for which Registration State Change Incidents are to be Generated** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
CS IP Address	Indicates the IP address of the Call Server in the field. This IP address specifies the Call Server IP address that includes the list of phones for which the registration state change incident must be generated .
Filter	Indicates the extension range to be included. For more information, see the Specifying the Range of Extensions for Nortel Phones to be Excluded from Monitoring.

4. Click **Add/Modify**. The **Current Configurations** section lists the configured Call Servers for which you want to generate the incident for registration state changes. You can select a CS IP address from the list and click **Modify** to modify the existing configuration. To delete an existing configuration, you can select a CS IP Address, and click **Delete**.

Configuring Polling

You can use the NNM iSPI for IP Telephony Nortel Polling Configuration form to enable polling and set intervals for the pollers that are grouped based on the Call Managers to be polled.

To configure the polling of a Call Manager, follow these steps:

1. On the NNM iSPI for IP Telephony Nortel Configuration console, click **Polling Configuration**. The NNM iSPI for IP Telephony Nortel Polling Configuration form opens.

2. In the **Call Manager Specific Polling Configuration** section, specify the required details in the fields provided on the page. The following table describes the fields on the page:

Field Name	Description
QOS Zones Monitoring	Allows you to configure the continuous polling of the various QOS-related measurements in the Nortel QOS Zones. The available options are as follows: ▪ Enable Polling: Select this check box to enable incident generation based on the values of the QOS metrics that are configured with the Nortel Signaling Server. ▪ Interval: Indicates the interval (in seconds) to poll the Nortel Signaling Sever to collect the details of QOS metrics. The default value is 300 seconds.
IP Phones Registration State Monitoring	Allows you to configure the continuous polling of the registration state of the Nortel IP Phones on the network. The available options are as follows: ▪ Enable Polling: Select this check box to enable the registration state of the Nortel IP Phones. ▪ Interval: Indicates the interval (in seconds) to poll the registration state of the Nortel IP Phones. The default value is 1800 seconds.

3. Click **Apply Changes**.

Extracting a Host Key

To extract an RSA level 2 host key for Avaya Communication Manager (CM), Cisco Unified Communications Manager (CUCM), and Acme Session Director (SD), follow these steps:

- **On Linux**

1. Make sure that no trusted host key is stored for the CM, CUCM, or SD in the Linux client machine at the following location:

   ```
   {home-dir}/.ssh/known_hosts
   ```

   To make sure of this, follow these steps:

   a. See the host keys present in the system by running the following commands:

      ```
      vi {home-dir}.ssh/known_hosts
      ```

      ```
      cat {home-dir}.ssh/known_hosts
      ```

The machine displays the list of host keys present in it.

A few examples of the host keys

```
nnmilxx ssh-rsa

AAAAB3NzaC1yc2EAAAABIwAAAQEA0QRT72TDI2FJ+VrVpNU8zTcdbz3gCyH2UFjqdU7Re9zT

Eq252Kzrrdriyvnaxhx4xcIHC+6iKjfF6UrEXAITon3mf1Ginp7AlBIpL6lgdkcKgH3VzjWtI
kx1dC0BEZa

HPseVP7PWy4RuSyyPbleql3O/Xltlm8MQPPYl3ZDeeQR07lxAU43685KK1w==

localhost ssh-rsa

AAAAB3NzaC1yc2EAAAABIwAAAQEA0QRT72TDI2FJ+VrVpNU8zTcdbz3gCyH2UFjqdU7Re9zTl

MuJf11RS4lyi0lXgZO4Yn7JsmT8BBDE11+zefB+si5vXTonpGfC/eOJr4HlM+73fdqVX1Br0t
ITxpoz3t

seVP7PWy4RuSyyPbleql3O/Xltlm8MQPPYl3ZDeeQR07lxAU43685KK1w==

192.168.15.14 ssh-rsa

AAAAB3NzaC1yc2EAAAABIwAAAIEArARKap4fSZLG0xkqT57TiftD34TCCrh5oIS6CQ6qfBmk0
uw

ANRx11g1mWppdNqIpT2+tHpn+sNN11JGV9IlnmxBnkdpyJFFNZwOK9dbB0glLY/ARuZOjJyb7
y5Jd

X0TYY+Sv6C9lcMzFLV8e5OBKJyxWSelQhvjJQTRzKPOKN+s=

192.168.16.17 ssh-rsa

AAAAB3NzaC1yc2EAAAABIwAAAQEArC1tF99fLtDQxAPoG+JLGnT10WWEtInB2w4SL3+Om6je9

iqBp0eL030O4hBs/et6ElZbKTo0kTbnXoopqiSKSrKtnjkxFcuXicOSxOFRPSqLin6BnLVsNg
uBU0ue

deYr8kOQDa/nGNwwp2lSqHTlHyzk1XiaLAglVg1yV92GISsgc36UAYomhGyF9piXPiQ==

nnmiwinxx,192.168.17.18 ssh-rsa

AAAAB3NzaC1yc2EAAAABIwAAAQEAu0Mi73QSqJrZ2jO5LPPwFZH+nECEfD3mEg0e5AEn8Jw68

zFiVtbmAXc0wshTeuW4dfo9OYKtqTxjWacye+ZgX7KvjSn9SATukQG1lp55bFhkSAuB46Y5Oj
qKpD+

8ud5FpipzbuUklqtzYAkzgD9bW+Z6pEBx2cA+lFV1NwQEuKUZCqhLFsbRsdvrJrw==

nnmiwinxx,192.168.19.21 ssh-rsa

AAAAB3NzaC1yc2EAAAABIwAAAQEA2YE67SaAeym4y73RW8Vc7bx3jnjRb4RqsqGr5YnI3cpf4
25D

Jv28ew4t+P7Bz+K78pFzbcaQtcwJZsNYc+MNVMXU39eS3b0fWDI0YlvexiUFAWlgH5bWiBioG
t2STdp

2WybstDHDfAS4VhBQLlMwe/pBY5Uj+pL0hXtds33abVR2bALD/96E2SQ==
```

```
iptnnmwinx,192.168.24.14 ssh-rsa

AAAAB3NzaC1yc2EAAAABIwAAAQEA0TdH+dc7OAUjehjTD6iwHshfGWUyydlA9BSyD9q4hZZOS
YU

VotByDGLONCfdhKqituAXEeXSbVxETingG1Kgzyu7UdO5T63xRwA3FtbJJbh1HK//p6hsk+cX
hQ32uB

+eGy6GnrJM543Yz0bIz7ipSm+DjqkhlNYtTV0wmmli3PozAW2sS8LOuo6LPQ==
```

b. Delete the entry that corresponds to the IP address of the CM, CUCM, or SD. For example, if the IP address of your CM, CUCM, or SD is 192.168.16.17, the host key that corresponds to the CM, CUCM, or SD may look like this:

192.168.16.17 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEArC1tF99fLtDQxAPoG+JLGnT10WWEtInB2w4S
L3+Om6je9deYr8kOQDa/nGNwwp2lSqHTlHyzk1XiaLAglVg1yV92GISsgc36UAYomhGy
F9piXPiQ==

2. Run an `ssh` command to the IP address of the remote CM, CUCM, or SD as follows:

```
ssh 192.168.16.17
```

The machine displays the following messages:

```
The authenticity of host '192.168.16.17 (192.168.16.17)' can't be establishe
d.

RSA key fingerprint is ba:40:95:5f:8c:ea:fb:ad:b5:97:5a:4e:d0:85:50.

Are you sure you want to continue connecting (yes/no)?
```

3. Note down the RSA key fingerprint as follows:

```
ba:40:95:5f:8c:ea:fb:ad:b5:97:5a:4e:d0:85:50
```

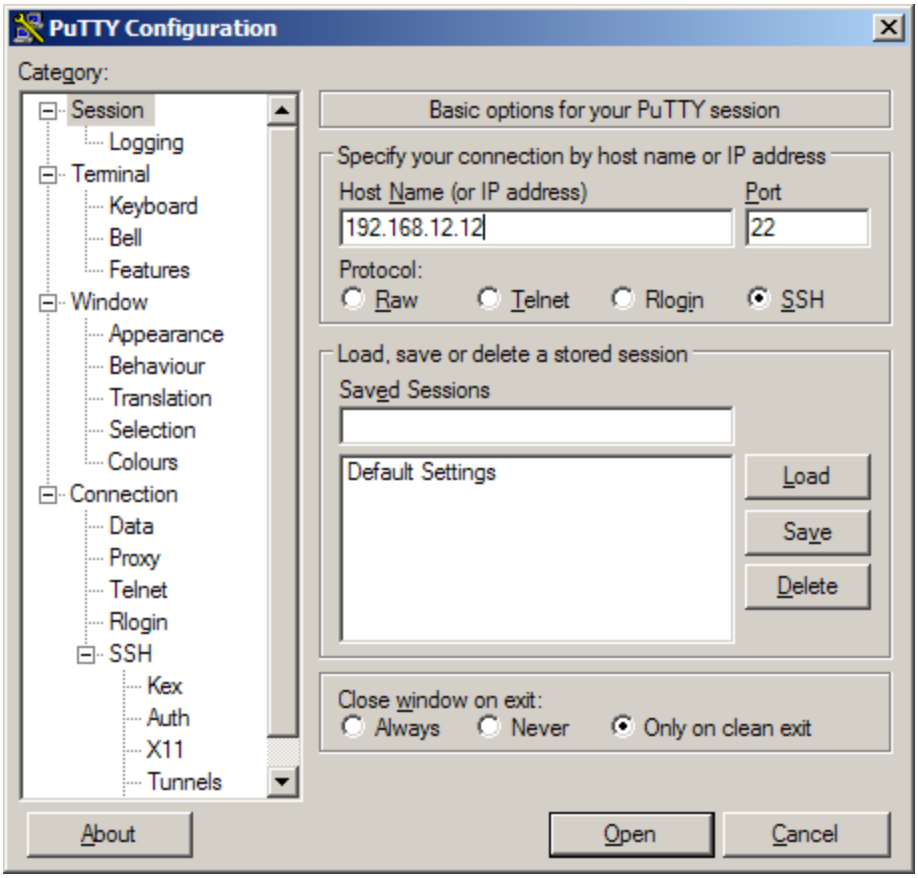
You can provide this RSA key in the Host Key field of the SSH configuration UI of the NNM iSPI for IP Telephony.

- **On Windows**

If you do not have a Linux client machine to extract the host key, you can extract a host key from a Windows machine using the PuTTY application or any other similar application.

To extract an RSA level 2 host key for the CM, CUCM, or SD using the PuTTY application, follow these steps:

1. Open the PuTTY application and type the host name or IP address of the CM, CUCM, or SD under the Host Name (or IP address) field .



2. Select **SSH** under the Protocol field.
3. Select **Only on clean exit** under the Close window on exit: field.
4. Click **Open**. A pop-up window opens:

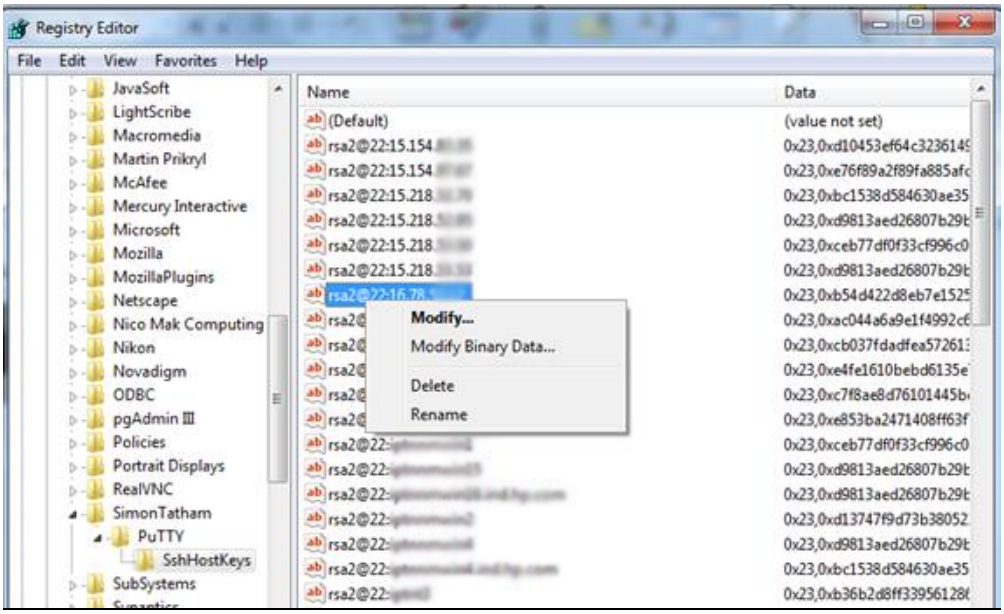
Note down the rsa2 key fingerprint and use it in the NNM iSPI for IP Telephony.

If the pop-up window does not open, it indicates that the host key for the IP address of the CM, CUCM, or SD is already cached in the registry by PuTTY in a previous session. In this scenario, you must clear the registry entry and repeat step 1 to step 4.

To clear the registry entry, follow these steps:

a. Browse to the following directory:

USER\Software\SimonTatham\PuTTY\SshHostKeys



b. Select and right-click the host key that corresponds to the IP address of the physical CM,CUCM, or SD.

c. Click **Delete**.

Note: To authenticate the server, make sure that a proper entry of the server exists in the **known_hosts** file (for example, `~/.ssh/known_hosts`) on the client machine. To achieve this, you must login to the remote server manually (using SSH) and make an entry into the **known_hosts** file.

Global IP Telephony Network Management

The NNM iSPI for IP Telephony along with NNMi helps you consolidate and manage IP telephony networks spread across different locations and managed by independent NNMi management servers (regional managers) through a single NNMi management server (global manager) console. You can add multiple regional managers to a global manager. This management capability provided by NNMi is referred to as the Global Network Management (GNM).

In a GNM scenario, from the global manager console, you cannot change the configuration settings or manage the IP telephony nodes that are managed by individual regional managers. The regional

managers manage the nodes associated with them and update the status of these nodes on the global manager console after the completion of each discovery cycle. Using the global manager, you can request for the status of a node that is managed by a regional manager. From the global manager console, you cannot add, edit, delete, or disable the monitoring settings for the entities managed by the regional managers.

Configuration Points

Note the following points that you must consider while setting up a GNM environment to manage your IP telephony networks:

- The regional manager does not replicate the threshold values configured for the nodes that they manage, on the global manager. You must therefore configure the threshold values again for these nodes on the global manager to achieve the desired management results.
- On the global manager console, the NNM iSPI for IP Telephony applies the phone exclusion filter specified for the global manager.
- The global manager performs a state polling on only the nodes that are managed by the global manager.
- The NNM iSPI for IP Telephony at the regional manager collects the CDR data for Avaya Communication Manager and Cisco Unified Communications Manager clusters from the Network Performance Servers (NPS) at the regional managers and updates the NPS at the global manager with this data for collective reporting.

For more information about GNM and setting up regional manager connections with a global manager, see the NNMi *Online Help* and the *NNMi Deployment Reference Guide*.

Related Topics:

- Regional Manager Configuration
- Adding a Regional Manager Configuration
- Modifying a Regional Manager Configuration
- Deleting a Regional Manager Configuration

Regional Manager Configuration

From the NNMi management server that you want to designate as the global manager, you can use the NNM iSPI for IP Telephony Regional Manager Configuration form to add, modify, or delete other NNMi management servers as regional managers.

To access the NNM iSPI for IP Telephony Regional Manager Configuration form:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...**. The HP NNM iSPI for IP Telephony Configuration Console opens.

2. Click **Regional Manager Configuration**. This opens the NNM iSPI for IP Telephony Regional Manager Configuration form.

The NNM iSPI for IP Telephony Regional Manager Configuration form displays the details of the regional managers currently configured with the global manager in the Configured Regional Managers table. The table displays the following details.

Regional Manager Attribute	Description
Name	The name of the regional manager.
Connection State	The connection state of the regional manager with the global manager. The possible connection states are as follows: • Not Established • Partial Connection • Connected • Not Connected See the *NNMi Online Help* for more information about the regional manager connection states.
Description	The description provided while configuring the regional manager.
UUID	The Universal Unique Identifier (UUID) of the regional manager.

Adding a Regional Manager Configuration

Before adding a regional network manager to the global network manager, see the *NNMi Online Help* for the prerequisites and any additional information required to configure a regional manager with a global manager.

To add a regional manager configuration, follow these steps:

1. From the NNMi console, click **Configuration** > **iSPI for IP Telephony Configuration...**. The HP NNM iSPI for IP Telephony Configuration Console opens.

2. Click **Regional Manager Configuration**. The NNM iSPI for IP Telephony Regional Manager Configuration form opens.

3. Click * (the **New** icon). The **Creating New Regional Manager** form opens, with the details displayed in two panels – the left panel and the right panel.

4. On the left panel, type the required **Name** and the **Description** for the regional manager in the respective boxes.

5. On the right panel, click (the **New** icon) displayed under the **Connections** tab. The **Add Regional Manager Connection** form opens.

   Note: You must configure at least one connection for a regional manager.

6. Specify the required details for the connection to the regional manager in the **Add Regional Manager Connection** form. You can configure multiple connections to a regional manager to support application failover. The following table describes the fields on the page:

Field Name	Description
Hostname	The official Fully-Qualified-Domain-Name (FQDN) of the Regional Manager.
Use Encryption	Select this check box to enable secure sockets layer encryption (HTTPS/SSL) to access this Regional NNMi management server. If disabled, NNMi uses hypertext transfer protocol (HTTP) and plain sockets to access this Regional NNMi management server.
HTTP(S) Port	The port number for HTTP or HTTPS access to the NNM iSPI for IP Telephony sever on the regional manager The default port numbers are as follows: ▪ HTTP: 10080 ▪ HTTPS: 10443. Type this value in the **HTTP(S) Port** box if you select **Use Encryption**. **Note:** If you are not using the default values for the ports, check the values that you configured from the `nms-ipt.ports.properties` file present in the `nnmDataDir\shared\ipt\conf` directory on the regional manager.
User Name	The user name required for NNMi to sign-in to the system account on this Regional NNMi management server.
Password	The password for the user name provided.
Ordering	The numeric value to define the order (lowest number first) in which NNMi checks for configuration settings. NNMi uses the first match found for each address. Provide a unique connection ordering number for each Regional Manager configuration.

7. Click (the **Save** icon) to add the new regional manager configuration.

8. Click (the **Refresh** icon) to view the newly-added regional manager configuration and its connection state.

Note: See the *NNMi Online Help* for more information about the regional manager connection details that you must specify to add a new regional manager.

Modifying a Regional Manager Configuration

The NNM iSPI for IP Telephony Regional Manager Configuration form allows you to modify the configuration details of an existing regional manager.

To modify the name and description of an existing regional manager, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...**. The HP NNM iSPI for IP Telephony Configuration Console opens.
2. Click **Regional Manager Configuration**. The NNM iSPI for IP Telephony Regional Manager Configuration form opens.
3. Select the regional manager from the **Configured Regional Managers** section and click **Open**. This opens the Modify Regional Manager Configuration form.
4. Update the **Name** and the **Description** for the regional manager in the respective boxes on the left panel.
5. Click **Save** to save the changes. This closes the Modify Regional Manager Configuration form and opens the NNM iSPI for IP Telephony Regional Manager Configuration form.

To modify the details of an existing regional manager connection, follow these steps:

1. Select the connection that you want to update from the **Connections** tab on the right panel and click **Open**. The Modify Regional Manager Connection form opens.

   Note: The NNM iSPI for IP Telephony does not allow you to modify an active connection. To modify an active connection to the regional manager, you must first stop the NNM iSPI for IP Telephony process on the active connection, wait for the application failover to complete (the NNM iSPI for IP Telephony connects using another configured connection to the regional manager based on the ordering number specified), and then update the connection details.

2. Update the required details in the fields on the form. For more information about the fields on the form, see Adding a Regional Manager Configuration.
3. Click (the **Save** icon) to save the modified settings for the regional manager configuration.

Deleting a Regional Manager Configuration

Before deleting a regional manager configuration, you must make sure that you have removed all the nodes associated with the regional manager. For more information about removing nodes

associated to a regional manager, see the *HP Network Node Manager i Software Online Help 10.00*.

To delete a regional manager configuration, follow these steps:

1. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration...**. The HP NNM iSPI for IP Telephony Configuration Console opens.
2. Click **Regional Manager Configuration**. The NNM iSPI for IP Telephony Regional Manager Configuration form opens.
3. Select the regional manager from the **Configured Regional Managers** section and click the **Open** icon. The Regional Manager Configuration form opens.
4. Select all the connections configured for the regional manager from the Connections tab page on the right panel and click **Delete**. This removes all the configured connections to the regional manager.

   Note: The NNM iSPI for IP Telephony does not allow you to delete an active connection to a regional manager. You can only delete inactive connections configured for a regional manager. To delete an active connection, you must stop the NNM iSPI for IP Telephony process running on the active connection and then delete the connection.
5. Click **Save**and return to the NNM iSPI for IP Telephony Regional Manager Configuration form.
6. Select the regional manager from the **Configured Regional Managers** section and click **Delete**.
7. Click **Save**. This completes the removal of the regional manager connection from the global manager.

Importing Configuration from the Regional Manager to the Global Manager

The (the **Import Monitoring Configuration, Monitoring Attribute States, and RTCP Reception Configuration** icon) on the **NNM iSPI for IP Telephony Regional Manager Configuration** form helps you to import the following from the regional network manager to the global network manager:

- Monitoring Configuration
- Monitoring Attribute Sates
- Avaya RTCP Reception Configuration

To import the Monitoring Configuration/Monitoring Attribute States/Avaya RTCP Reception Configuration, follow these steps:

1. From the NNMi console, click **Configuration** > **iSPI for IP Telephony Configuration**. The IP Telephony Configuration console opens.
2. Click **Regional Manager Configuration**. The **NNM iSPI for IP Telephony Regional Manager Configuration** form opens.
3. From the **Configured Regional Managers** table, select the regional network manager configuration that you want to export to the global network manager, and then click . The NNM iSPI for IP Telephonyexports the selected Monitoring Configuration/Monitoring Attribute States/Avaya RTCP Reception Configuration to the global network manager.

Managing the Lifecycle of NNMi Nodes Hosting IP Telephony Devices

You can manage the lifecyle of the NNMi nodes that host the IP Telephony services such as Cisco Voice Gateway, Cisco Unified Communications Manager, Avaya Media Gateway, and Avaya Communications Manager using the NNMi console.

To manage the lifecycle of NNMi nodes that host the IP Telephony services, follow these steps:

1. From the navigation pane, clcik **Inventory** > **Nodes**.
2. , select the IP telephony device that you want to start or stop monitoring.
3. Click **Actions** > **Management Mode**. Select one of the following options:
   - **Manage**: Monitors the status of the selected node.
   - **Manage (Reset All)**: Specifies that the selected node and the interfaces and devices registered with the selected node must be monitored. The interfaces and devices inherit the management status of the selected node.
   - **Not Managed**: Specifies that the selected node must not be monitored. After you select this option, the NNM iSPI for IP Telephony stops monitoring the status of the selected node.
   - **Out of Service**: Specifies that the selected node is out of service. After you select this option, the NNM iSPI for IP Telephony stops monitoring the status of the selected node.

You can manage the discovery and monitoring of the following IP Telephony devices:

- Cisco
  - Call controllers
  - Voice gateways

- Gatekeepers
- Unity devices
- IP phones

- Avaya
  - Primary server
  - Media gateway
  - CLAN
  - IPSI
  - Media processor
  - LSP
  - IP phones

Managing Cisco IP Telephony Devices

See the following table to know more about the effects of keeping your Cisco IP telephony devices in the **Out of Service** or **Not Managed** modes:

IP Telephony Device	Action—Result
Call Controller	Out of Service: • Marks the status of the call controller as not monitored • Stops polling the call controller for the status • Changes the registration state of the phones associated with the call controller as unknown • Changes the management state of the call controller in the Call Controller form to Out of Service Not Managed: • Marks the status of the call controller as not monitored • Stops polling the call controller for the status • Changes the registration state of the phones associated with the call controller as unknown • Changes the management state of the call controller in the Call Controller form to unmanaged.
Voice Gateway	Out of Service: • Marks the status of the voice gateway as not monitored. • Stops polling the voice gateway for the status • Changes the management state of the voice gateway in the node form to out of service Not Managed: • Marks the status of the voice gateway as not monitored. • Stops polling the voice gateway for the status • Changes the management state of the voice gateway in the node form to unmanaged

IP Telephony Device	Action—Result
Gatekeeper	Out of Service: • Marks the status of the gatekeeper as not monitored. • Stops polling the gatekeeper for the status • Changes the number of registered endpoints for the gatekeeper to not monitored. • Changes the management state of the gatekeeper in the node form to out of service Not Managed: • Marks the status of the gatekeeper as not monitored. • Stops polling the gatekeeper for the status • Changes the management state of the gatekeeper in the node form to unmanaged
Unity Device	Out of Service: • Marks the status of the unity device as not monitored. • Changes the management state of the gatekeeper in the node form to out of service Not Managed: • Marks the status of the unity device as not monitored. • Changes the management state of the gatekeeper in the node form to unmanaged

IP Telephony Device	Action—Result
IP Phone	Out of Service: • Marks the status of the phone as not monitored. • Stops polling the phone for the status • Changes the management state of the phone in the extension details form to out of service Not Managed: • Marks the status of the phone as not monitored. • Stops polling the phone for the status. • Changes the management state of the phone in the extension details form to unmanaged

Note: When you mark the status of an IP telephony device that has registered devices or associated interfaces to out of service or not managed, only the registration state of the associated devices change to unknown. The NNM iSPI for IP Telephony still continues to poll the registered devices or associated interfaces for the status till you specifically mark the status of these devices to out of service or not managed.

Managing Avaya IP Telephony Devices

See the following table to know more about the effects of keeping your Avaya IP telephony devices in the **Out of Service** or **Not Managed** modes:

IP Telephony Device	Action—Result
Primary server	Out of Service: • Marks the status of the primary server as not monitored • Stops polling the primary server for the status • Changes the registration state of the phones associated with the call controller as unknown • Changes the management state of the call controller in the Call Controller form to Out of Service • Stops the discovery of associated primary server entities such as the network region, the route pattern, the trunk group, and so on Not Managed: • Marks the status of the primary server as not monitored • Stops polling the primary server for the status • Changes the registration state of the phones associated with the call controller as unknown • Changes the management state of the call controller in the Call Controller form to unmanaged • Stops the discovery of associated primary server entities such as the network region, the route pattern, the trunk group, and so on
Media Gateway	Out of Service: • Marks the status of the media gateway as not monitored. • Stops polling the media gateway for the status • Changes the management state of the voice gateway in the Media Gateway Detailed form to out of service Not Managed: • Marks the status of the media gateway as not monitored. • Stops polling the media gateway for the status • Changes the management state of the media gateway in the Media Gateway Detailed form to unmanaged

IP Telephony Device	Action—Result
LSP	Out of Service: • Marks the status of the LSP as not monitored. • Stops polling the LSP for the status • Changes the management state of the LSP in the Call Controller form to out of service Not Managed: • Marks the status of the LSP as not monitored. • Stops polling the LSP for the status • Changes the management state of the LSP in the Call Controller form to unmanaged
CLAN, IPSI, or Media Processor	Out of Service: • Marks the status of the device as not monitored. • Stops polling the device for the status • Changes the management state of the device in the corresponding detail form to out of service Not Managed: • Marks the status of the device as not monitored. • Stops polling the device for the status • Changes the management state of the device in the corresponding detail form to unmanaged

IP Telephony Device	Action—Result
IP Phone	Out of Service: • Marks the status of the phone as not monitored. • Stops polling the phone for the status • Changes the management state of the phone in the phone details form to out of service Not Managed: • Marks the status of the phone as not monitored. • Stops polling the phone for the status. • Changes the management state of the phone in the phone details form to unmanaged

Note: When you mark the status of an IP telephony device that has registered devices or associated interfaces to out of service or not managed, only the registration state of the associated devices change to unknown. The NNM iSPI for IP Telephony still continues to poll the registered devices or associated interfaces for the status till you specifically mark the status of these devices to out of service or not managed.

Deleting IP Telephony Entities from the NNM iSPI for IP Telephony

You can delete the IP Telephony entities that you do not want to monitor by deleting the NNMi node objects that host these entities.

To delete the NNM iSPI for IP Telephony entities from the NNMi node inventory, follow these steps:

1. Select the IP telephony device that you want to delete from the **Inventory** > **Node** > Node - Nodes view.
2. Click **Actions** > **Delete** from the menu on the NNMi console. This deletes the selected IP telephony device from the NNM node inventory.

Deleting the hosted IP Telephony entities by deleting the NNMi node objects that host these entities from the NNMi node inventory also removes the association of these entities. For example, if you remove a node hosting the Avaya primary controller (Avaya Communications Manager), the NNM iSPI for IP Telephony removes the corresponding NNM iSPI for IP Telephony Call Controller entity along with all the references in the NNM iSPI for IP Telephony media gateway entities for this

primary controller, the associated CLAN, IPSI, and media processor, the port network, the IP network region, and so on in the NNM iSPI for IP Telephony.

Note: You can use the NNM iSPI for IP Telephony Phone Exclusion Configuration form to delete a large number of Cisco IP Phone or Avaya IP Phone entities in the NNM iSPI for IP Telephony without having to delete the Cisco Unified Communications Managers or the Avaya Communications Manager nodes in NNMi or without having to delete batches of NNMi nodes hosting the IP Phones.

Configuring Processing of Traps Sent by Nortel Call Server

The NNM iSPI for IP Telephony by default processes traps sent by the Nortel Call Server that carry only the message codes that belong to the following message code categories. The NNM iSPI for IP Telephony ignores other message codes and does not display the corresponding incidents on the incident browser.

- ITG
- ITS
- QOS

Note: A message code category represents a group of message codes that relate to the same entity. A message code category is represented by the initial alphabets that constitute the message code. Message codes and error codes refer to the same entity in the context of traps.

To configure the NNM iSPI for IP Telephony to process traps that contain message codes that you require, follow these steps:

1. Open the `NortelCSMessageCodes.conf` file present in the following directory:
   - For non Windows platforms: `NNM_DATA_DIR/shared/ipt/conf`. NNM_DATA_DIR represents the data directory in your system after you have installed NNMi.
   - For Microsoft Windows platforms: NNM_DATA_DIR\shared\ipt\conf
2. If you want the NNM iSPI for IP Telephony to process all the traps sent by the Nortel Call Server, remove the pound sign (#) from the `ENABLE_ALL` entry in the file. This uncomments the `ENABLE_ALL` entry.
3. If you want the NNM iSPI for IP Telephony to process specific traps sent by the Nortel Call Server, you can add the message code or the message code category in the `NortelCSMessageCodes.conf` file. You must add each entry as a separate line in the file. Note that to specify a message code category, you must specify the message code without the numeric part or the first three letters of the message code.
4. Restart the `ovjboss` process to apply the changes.

Note: To disable the processing of traps, you can rename, delete, or move the `NortelCSMessageCodes.conf` file.

NNM iSPI for IP Telephony Logging

To monitor the health, performance, and availability of different NNM iSPI for IP Telephony processes, you can view the log files (`ipt-trace` and `ipt`) that are stored in the following directory:

On the UNIX management server: `/var/opt/OV/log/ipt`

On the Windows management server: `%NnmDataDir%\log\ipt`

The `ipt` file provides a log of all errors and warnings triggered by different processes and components of the iSPI. The `ipt-trace` file shows the information that helps you trace those errors and warnings.

The `jboss-logging.xml` file enables you to configure different logging levels for different processes and components of the NNM iSPI for IP Telephony. You can specify the maximum size of the log and trace files with the help of the `jboss-logging.xml` file. The `jboss-logging.xml` file lists all components in the form of XML elements in the following format:

```
<logger category="fully_qualified_component_name"> <level name="log_level"/>
</logger>
```

In this instance:

fully_qualified_component_name is the fully qualified package name of the component or process.

log_level is the logging level.The NNM iSPI for IP Telephony supports the following levels of logging:

- **INFO:** Logs only the messages generated by different components and processes of the NNM iSPI for IP Telephony
- **FINE:** Shows the root of the problem along with logging messages
- **FINEST:** Logs the most comprehensive level of details

By default, all components are set to INFO.

To set the logging level, follow these steps:

1. Open the `jboss-logging.xml` file with a text editor from the following location on the management server:
   - On UNIX/Linux: `/var/opt/OV/shared/ipt/conf`
   - On Windows: `%NnmDataDir%\shared\ipt\conf`
2. Configure the logging level.

Set `level name` to INFO, FINE, or FINEST for each NNM iSPI for IP Telephony component. Table: Components in the jboss-logging.xml File provides you with a list of NNM iSPI for IP Telephony components presented in the `jboss-logging.xml` file:

Table: Components in the jboss-logging.xml File

Component	Logger Category in the jboss-logging.xml File
NNM iSPI for IP Telephony services	com.hp.ov.nms.spi.ipt.services
NNM iSPI for IP Telephony services	com.hp.ov.nms.spi.uc.services
NNM iSPI for IP Telephony discovery	com.hp.ov.nms.spi.ipt.disco
NNM iSPI for IP Telephony discovery	com.hp.ov.nms.spi.uc.disco
NNM iSPI for IP Telephony state poller	com.hp.ov.nms.spi.ipt.statepoller
NNM iSPI for IP Telephony state poller services	com.hp.ov.nms.spi.ipt.services.statepoller
NNM iSPI for IP Telephony state poller notification in a Global Network Management environment	com.hp.ov.nms.statepoller.notification.state.geo
CDR/CMR monitoring and reports	com.hp.ov.nms.spi.ipt.cdr.cisco.collection
NNM iSPI for IP Telephony discovery notification	com.hp.ov.nms.spi.ipt.disco.notification
	com.hp.ov.nms.spi.ipt.rtcp
	com.hp.ov.nms.spi.ipt.monitoring.impl.services
	com.hp.ov.nms.spi.ipt.monitoring.services

3. Configure the maximum size of a log file.

   a. Go to the `size-rotating-file-handler` element for the `ipt` file in the `jboss-logging.xml` file.

   b. Configure the following attributes:
      - autoflush: Set it to true if you want the iSPI to delete log files automatically after the file size reaches the upper limit.
      - rotate-size: Set it to the value `"${com.hp.ov.nnm.log.trace.size,com.hp.ov.nnm.log.size:<size>M}"` where <*size*> is the maximum size of the log file in MB. After the `ipt` file size reaches the specified MB, the NNM iSPI for IP Telephony archives the log file and creates a fresh `ipt` file. The NNM iSPI for IP Telephony creates the following archived file:

`ipt.log.<n>`

In this instance, n is an integer

- max-backup-index: Set it to the value `"${com.hp.ov.nnm.log.trace.count,com.hp.ov.nnm.log.count:<n>M}"` where *<n>* is the maximum number of the archived log files that can be present in the directory. After the total number of `ipt.log` files exceeds the specified value, the NNM iSPI for IP Telephony deletes the oldest archive file.

c. Go to the `size-rotating-file-handler` element for the `ipt-trace` file in the `jboss-logging.xml` file.

d. Repeat step b.

4. Save the file. The modified logging behavior takes effect immediately.

Integration with ClarusIPC

You must make sure that you have a valid license for the HP NNM iSPI Network Engineering Toolset before enabling the integration of NNM iSPI for IP Telephony with Clarus IPC. This is an optional integration that you can enable after installing the NNM iSPI for IP Telephony.

To integrate the NNM iSPI for IP Telephony with ClarusIPC, follow these steps:

1. Log on to the NNMi console with the administrative privileges.
2. In the Workspaces pane, click **Integration Module Configuration > NNM iSPI for IP Telephony-ClarusIPC Integration**. The HP NNMi-ClarusIPC Integration Configuration window opens.
3. Select the **Enable Integration** option.
4. Specify the following details:
   - Clarus Host: IP address or hostname of the ClarusIPC server.
   - Clarus Port: Port number of the ClarusIPC server.
   - NNM Admin User: The user name of an NNMi user with the administrative privileges.
   - NNM Admin Password: The password of the above user.
5. Click **Submit**.

After you enable the integration, new workspaces appear in the Workspaces pane and new URL actions appear in the Actions menu of the Cisco IP Phones view and the incident browser.

If additional URL actions do not appear in the **Actions** menu of the Cisco IP Phones view or the incident browser, stop and start all NNMi processes with the **ovstop** and **ovstart** commands. If the URL actions still do not appear, run the **ovstop** and **ovstart** commands again.

If you want to disable the ClarusIPC integration, go to the HP NNMi-ClarusIPC Integration Configuration window, clear the **Enable Integration** option, and then click **Submit**.

After you disable the integration, all ClarusIPC-specific forms and menu items must disappear. If the ClarusIPC-specific menu items continue to appear in the Actions menu, stop and start NNMi processes with the **ovstop** and **ovstart** commands.

Before you remove the NNM iSPI for IP Telephony from the system, make sure to perform the following tasks:

1. Disable the ClarusIPC integration.
2. Remove all the patches for the NNM iSPI for IP Telephony.

We appreciate your feedback!

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Online Help (Network Node Manager iSPI for IP Telephony Software 10.00)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to docfeedback@hp.com.