

HP Network Node Manager iSPI for IP Telephony Software

For the HP-UX, Solaris, and Linux operating systems

Software Version: 9.21

Online Help

Document Release Date: June 2013

Software Release Date: June 2013



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 2008-2013 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

Disclaimer for 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.

Note: Some topics do not convert properly to PDF, causing format problems. Some elements of online help are completely removed from the PDF version. Those problem topics can be successfully printed from within the online help.

Contents

Online Help.....	1
Oracle Technology — Notice of Restricted Rights.....	2
Acknowledgements.....	2
Contents.....	7
HP Network Node Manager iSPI for IP Telephony Software.....	16
Managing the IP Telephony Network.....	16
Discovering IP Telephony Networks.....	17
Discover IP phones.....	17
NNM iSPI for IP Telephony Quick Start Wizard.....	17
NNM iSPI for IP Telephony Quick Start Wizard for Avaya.....	18
Primary Communication Manager Server.....	19
SNMP Configuration.....	19
Switch Administration Terminal Configuration.....	19
Extracting a Host Key for the Avaya Communication Manager and Cisco ... Unified Communications Manager.....	20
CDR Access Configuration.....	23
Obtaining CDR Configuration Parameters from the Avaya Communication Manager.....	24
Creating a Customized File.....	30
RTCP Configuration.....	32
Obtaining RTCP Configuration Parameters from the Avaya Communication Manager.....	32
Summary.....	33
NNM iSPI for IP Telephony Quick Start Wizard for Cisco.....	34
UCM Publisher.....	34
AXL Configuration.....	34
SNMP Configuration.....	34
SSH Configuration.....	35

Extracting a Host Key for the Avaya Communication Manager and Cisco ... Unified Communications Manager.....	36
CDR Access Configuration.....	39
Summary.....	40
Help for Operators.....	40
IP Telephony Inventory.....	41
Monitoring Cisco Unified Communications Manager Clusters.....	41
Filtering UCM Clusters.....	44
UCM Cluster Details Form.....	44
Monitoring UCM Subscriber Groups.....	45
UCM Subscriber Group Details Form.....	47
Monitoring Cisco Unified Communications Managers.....	48
Cisco Call Controller Details Form.....	50
Monitoring Device Pools.....	54
Device Pool Details Form.....	56
Monitoring H.323 Gateways.....	58
Viewing Cisco Voice Gateway Details Form.....	61
Monitoring MGCP/SCCP Gateways.....	62
Voice Gateway Interface Details Form.....	65
Voice Gateway Channels Details Form.....	67
Monitoring SRST Routers.....	67
Cisco Call Controller Details Form.....	69
Monitoring IC Trunks.....	73
H323 Trunk Details Form.....	75
Monitoring Media Devices.....	76
Media Device Details Form.....	78
Monitoring Voice Mail Devices.....	79
Monitoring UCMEs.....	80
Filtering UCMEs.....	81
Cisco Call Controller Details Form.....	82
Monitoring IP Phones.....	86
Filtering Cisco IP phones.....	88

Cisco Extension Details form.....	89
Updating Site Codes, Mail Codes, and Location Details of Cisco IP Phones.....	90
Monitoring Cisco Gatekeepers.....	91
Filtering Cisco Gatekeepers.....	92
Cisco GateKeeper Details Form.....	93
Monitoring Cisco Unity Devices.....	94
Filtering Cisco Unity Devices.....	95
Cisco Unity Devices Form.....	95
Monitoring Configuration for Cisco Unified Communications Manager Clusters and Cisco Unified Communications Managers.....	96
Monitor Call Activities.....	97
Enable Call Activity Monitoring.....	97
Select Call Activities for Monitoring.....	99
Monitoring Registered Devices Count.....	100
Enable Registered Devices Count Monitoring.....	102
Configuring Registered Devices Count Settings.....	103
Configure Cisco TFTP Server Monitoring.....	105
Configure Cisco TFTP Server Monitoring Settings.....	107
Configure Route List and Hunt List Count Monitoring.....	109
Configuring Route List and Hunt List Count Settings.....	111
Configure Media Resource Activity Monitoring.....	112
Configuring Media Resource Activity Monitoring Settings.....	114
Configure Gateway Call Activity Monitoring.....	116
Configuring Gateway Call Activity Monitoring Settings for a Cluster.....	118
Configuring Gateway Call Activity Monitoring for a Gateway Interface.....	118
Configure Monitoring of the Call Manager Administration Web Page.....	
Availability.....	120
Configure Monitoring of Call Manager Administration Web Page State.....	
Settings.....	121
Monitor the Health of Cisco Unified Communications Managers.....	122
Enable Monitoring.....	123
Select System Health Parameters for Monitoring.....	123
Configure Monitoring of Availability of Services on the UCM.....	125

Settings for Availability of Services on the UCM.....	127
Guidelines.....	128
ClarusIPC Integration—Test Plans and Test Result Reports.....	128
Viewing Route Group P.01 Grade of Service Summary Report.....	129
Viewing Route List P.01 Grade of Service Summary Report.....	131
Monitoring Nortel Call Servers.....	132
Filtering Nortel Call Servers.....	134
Nortel Call Server form.....	134
Monitor Nortel Signaling Servers.....	135
Filtering Nortel Signaling Servers.....	136
Nortel Signaling Server Details Form.....	137
Nortel QOS Zones Table View.....	138
View the Nortel QOS Zone Details form.....	138
Filtering Nortel QOS Zones.....	138
View the Nortel QOS Zone Details Form.....	139
Nortel IP Phones View.....	141
Filtering Nortel IP phones.....	142
Nortel Phone Detailed form.....	142
Monitoring Nortel Media Gateways.....	143
Filtering Nortel Media Gateways.....	144
View the Nortel Media Gateway Details Form.....	145
Monitoring Avaya Call Controllers.....	145
Filtering Avaya Call Controllers.....	148
Avaya Call Controller Details Form.....	149
Monitoring Network Regions.....	151
Filtering Avaya Network Regions.....	153
IP Network Region Detail Form.....	154
Monitoring IP Media Processor DSP Resource Metrics.....	156
IP Network Region Connection Detail Form.....	158
Monitoring Route Patterns.....	159
Filtering Avaya Route Patterns.....	160

Route Pattern Details Form.....	161
Monitoring Trunk Group Usage.....	163
Monitoring Trunk Groups.....	163
Filtering Avaya Trunk Groups.....	165
Trunk Group Detailed Form.....	166
Monitoring Trunk Group Members.....	168
Trunk Group Member Detailed Form.....	169
Monitoring Signaling Groups.....	169
Signaling Group Details Form.....	171
Monitoring Processor Occupancy Metrics.....	171
Filtering Avaya Port Networks.....	174
Port Network Detail Form.....	175
Monitoring IP Server Interface.....	176
IP Server Interface Details Form.....	178
Monitoring CLAN.....	179
CLAN Details Form.....	180
Monitoring Media Processors.....	182
Media Processor Details Form.....	184
Monitoring Port Network Load Details Metrics.....	186
Monitoring Total Load Metrics.....	187
Monitoring Intercom Load Metrics.....	188
Monitoring Incoming Trunk Load Metrics.....	189
Monitoring Outgoing Trunk Load Metrics.....	189
Monitoring Tandem Trunk Load Metrics.....	190
Monitoring Avaya IP Phones.....	190
To launch the Avaya IP Phones view:.....	190
Filtering Avaya IP phones.....	192
Avaya IP Phones Details Form.....	193
Monitoring Media Gateways.....	194
Filtering Avaya Media Gateways.....	196

Media Gateway Details Form.....	197
Monitoring Media Modules.....	199
Filtering Avaya Media Modules.....	200
Media Modules Form.....	201
Monitoring VOIP Engines.....	201
Filtering Avaya VOIP Engines.....	203
VOIP Engines Form.....	204
Monitoring DSP Cores.....	205
Filtering Avaya DSP Cores.....	206
DSP Cores Form.....	207
Incidents Collected from the ClarusIPC Environment.....	207
Context-Sensitive URLs for ClarusIPC Incidents.....	208
Incidents Generated by the NNM iSPI for IP Telephony.....	209
View SNMP Traps for Avaya Maintenance Objects.....	234
Incidents for Avaya Devices.....	235
Viewing Network Connectivity.....	236
Viewing the Graph for Jitter.....	237
Viewing the Graphs for Average Packet Loss.....	237
Viewing the Graph for the Average MOS.....	237
Viewing the Graphs for Latency.....	238
Launch a Voice Path.....	238
Launch a Control Path.....	239
Launch the HTTP to Phone Path.....	239
Integration with the iSPI Performance for Quality Assurance.....	240
Integration with the iSPI Performance for Traffic.....	240
Help for Administrators.....	241
Specify the Range of Extensions for Cisco, Avaya, and Nortel Phones to be Excluded from Monitoring.....	242
Configuring Data Access.....	245
Configuring Data Access for Cisco.....	245
Configure the NNM iSPI for IP Telephony to Access the AXL Data.....	246
Access the CDR Data.....	247

Prerequisites.....	247
Configure the NNM iSPI for IP Telephony to Access the CDR Data.....	250
Access the Cisco Unified Communications Manager with SSH.....	254
Configuring Data Access for Avaya.....	255
Creating Customized CDR Format Specification Files.....	258
Configuring RTCP Reception.....	259
Configuring SSH Access for Avaya.....	261
Configuring Data Access for Nortel.....	262
Extracting a Host Key for the Avaya Communication Manager and Cisco Unified Communications Manager.....	264
Configuring Monitoring Tasks.....	267
Configuring Monitoring Tasks Related to Cisco IP Telephony.....	267
Configuring the QOS and MOS Monitoring Threshold Values for Cisco.....	267
Configuring Cluster-Specific QOS and MOS Monitoring Threshold Values..	268
Configure Call Termination Cause Codes to be Monitored.....	269
Configure the Monitoring for Registration State and Call Manager Association of IP Phones.....	270
Specifying the List of IP Phones for Registration State Change Incident Generation.....	271
Configure the Monitoring of Call Managers.....	271
Configure the Monitoring of Voice Gateway Channels.....	272
Configure the Monitoring of Voice Gateway Interfaces.....	273
Configure the Monitoring of Gatekeepers.....	274
Configure the Monitoring of Call Manager Voice Mail Devices.....	275
Configuration for Survivable Remote Site Telephony (SRST) Monitoring.....	275
Configure the Monitoring of License Consumption for Unity Devices and Unity Connection Servers.....	276
Configuring Monitoring for Avaya IP Telephony Devices.....	276
Configure the Monitoring for CLAN and IP Phone Association.....	277
Configure the Monitoring for IP Phones.....	277
Specifying the List of IP Phones for Registration State Change Incident Generation.....	278
Configure the Monitoring for Media Processors.....	278

Configure the Monitoring for IP Server Interfaces.....	279
Configure the Monitoring for IP Network Regions.....	279
Configure the State Monitoring for the Duplex Primary Servers.....	280
Configure the State Monitoring for Survivable Servers.....	280
Configure the Monitoring for Media Gateways.....	281
Configure the Monitoring for Route Pattern Usage Metrics.....	282
Configure the Monitoring for Trunk Groups.....	283
Configure the Monitoring for Port Network Load Statistics.....	284
Configure the Monitoring for Processor Occupancy Statistics.....	284
Configuring Monitoring Tasks for Nortel IP Telephony.....	285
Configuring QoS Zones Monitoring.....	285
Configure the Monitoring of IP Phones.....	285
Specifying the List of IP Phones for Registration State Change Incident Generation.....	286
Reporting Configuration.....	286
Configure Cisco IP Telephony CDR-based Reporting.....	287
Enabling Cisco B-Channel Activity Reports.....	287
Enabling Phone MAC Reports.....	288
Enabling Voice Mail Reports.....	289
Configure Avaya IP Telephony Reporting.....	290
Enabling Trunk Activity Reports.....	290
Enabling Trunk Group Usage Reports.....	291
Enabling Processor Occupancy Summary Reports.....	291
Enabling Port Network Load Reports.....	291
Enabling Phone MAC Reports.....	292
Enabling IP Network Region DSP/Codec Summary Report.....	294
Enabling Route Pattern Usage Report.....	294
Global IP Telephony Network Management.....	294
Configuration Points.....	295
Regional Manager Configuration.....	295
Adding a Regional Manager Configuration.....	296
Modifying a Regional Manager Configuration.....	297

Deleting a Regional Manager Configuration	298
Configuring Discovery and Custom Attributes Settings	299
Configuring Discovery Settings for Avaya Primary Servers	299
Configuring Discovery Cycle for Avaya Primary Servers	299
Configuring Custom Attributes Settings for Avaya IP Phones	301
Configuring Custom Attributes Settings for Cisco IP Phones	301
Managing the Lifecycle of NNMi Nodes Hosting IP Telephony Devices	301
Managing Cisco IP Telephony Devices	302
Managing Avaya IP Telephony Devices	304
Deleting IP Telephony Entities from the iSPI for IP Telephony	306
Configuring Processing of Traps Sent by Nortel Call Server	307
NNM iSPI for IP Telephony Logging	308
To set the logging level:	308
Integration with ClarusIPC	310

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.

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.

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 the 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.

NNM iSPI for IP Telephony Quick Start Wizard

The NNM iSPI for IP Telephony Quick Start Wizard enables the administrators to configure the NNM iSPI for IP Telephony to monitor and manage the IP Telephony infrastructure in your network environment.

To configure the NNM iSPI for IP Telephony Quick Start Wizard, follow these steps:

1. Log on to the NNM iSPI for IP Telephony Quick Start Wizard using the `system` account that you created when installing NNMi.
2. Click **Login**. The Vendor Selection page opens.

3. Specify the following details on the Vendor Selection page.
 - **Vendor Name:** Select the name of the IP Telephony vendor whose devices you want to manage using the NNM iSPI for IP Telephony.
 - **External IP Address:** Type the external or public IP address of the NNMi server.
4. Click **Next**.
 - If you select Avaya as vendor, the [Primary Communication Manager Server](#) page opens.
 - If you select Cisco as vendor, the [UCM Publisher](#) page opens.

Click **Log Out** to log out of the NNM iSPI for IP Telephony Quick Start Wizard and return to the Login page.

Configuring Quick Start Wizard to use PKI-based authentication

The NNM iSPI for IP Telephony Quick Start Wizard is configured to use the credential-based authentication. However, you can configure the NNM iSPI for IP Telephony Quick Start Wizard to use the 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*
`%nnminstallldir%\bin\nmsiptauthconfigreload.ovpl`
 - On UNIX/Linux*
`/opt/OV/bin/nmsiptauthconfigreload.ovpl`

NNM iSPI for IP Telephony Quick Start Wizard for Avaya

You can use the NNM iSPI for IP Telephony Quick Start Wizard for Avaya to configure the NNM iSPI for IP Telephony to access management data from the Avaya IP Telephony servers in your environment.

Primary Communication Manager Server

Specify the following details on the Primary Communication Manager Server page:

- **Server Type:** Select the primary communication manager server type.
Select Duplex if the Avaya Communication Manager is running on a duplex redundant pair.
- **Physical Server IP:** Enter the IP address of the primary communication manager server.
If the Server Type is Duplex, do not use the Active IP or the Virtual IP of the duplex redundant pair.
- **Duplicate Physical Server IP:** If the Server Type is Duplex, enter the IP address of the duplicate physical server.

Click **Next**. The [SNMP Configuration](#) page opens.

SNMP Configuration

Specify the following details on the SNMP Configuration page:

- **Physical Server IP:** Specifies the IP address of the communication manager. This field is populated by default.
- **Community String:** Type the SNMP community string of the communication manager server.
Make sure that the community string configured on the physical communication manager server is same for SNMPv1 and SNMPV2c.

Click **Next**. The [Switch Administration Terminal \(SAT\) Configuration](#) page opens.

Click **Test** to initiate an SNMP communication test on the physical server.

Click **Previous** to return to the [Primary Communication Manager Server](#) page.

Switch Administration Terminal Configuration

Specify the following details on the Switch Administration Terminal (SAT) Configuration page:

- **Physical Server IP:** Specifies the IP address of the communication manager. This field is populated by default.
- **Username:** Type the SSH user name to log on to the primary communication manager server.
- **Password:** Type the password for the SSH user name specified above.
- **Port:** Specifies the port number on the primary communication manager server to which SSH connections can be established from the NNM iSPI for IP Telephony server. This field is populated by default.
- **Timeout (secs):** Specifies the number of seconds to wait while attempting to run a command before canceling the attempt and generating an error. This field is populated by default.
- **Host Key:** Type the RSA Level2key host key of the primary communication manager server.
For details on extracting host key, see [Extracting a Host Key for the Avaya Communication Manager and Cisco Unified Communication Manager](#).

Click **Next**. The [CDR Access Configuration](#) page opens.

Click **Test** to test the SAT configuration.

Click **Previous** to return to the [SNMP Configuration](#) page.

Extracting a Host Key for the Avaya Communication Manager and Cisco Unified Communications Manager

To extract an RSA level 2 host key for Avaya Communication Manager (CM) or Cisco Unified Communications Manager (CUCM), follow these steps:

- **On UNIX/Linux**

1. Make sure that no trusted host key is stored for the CM or CUCM 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.

- b. Delete the entry that corresponds to the IP address of the CM or CUCM. For example, if the IP address of your CM or CUCM is 192.168.16.17, the host key that corresponds to the CM or CUCM may look like this:

```
192.168.16.17 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEARC1tF99fLtDQxAPoG+JLGnT10WWEtInB2w4SL3+Om6je9deYr8k
```

2. Run an `ssh` command to the IP address of the remote CM or CUCM 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
established.
```

```
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.

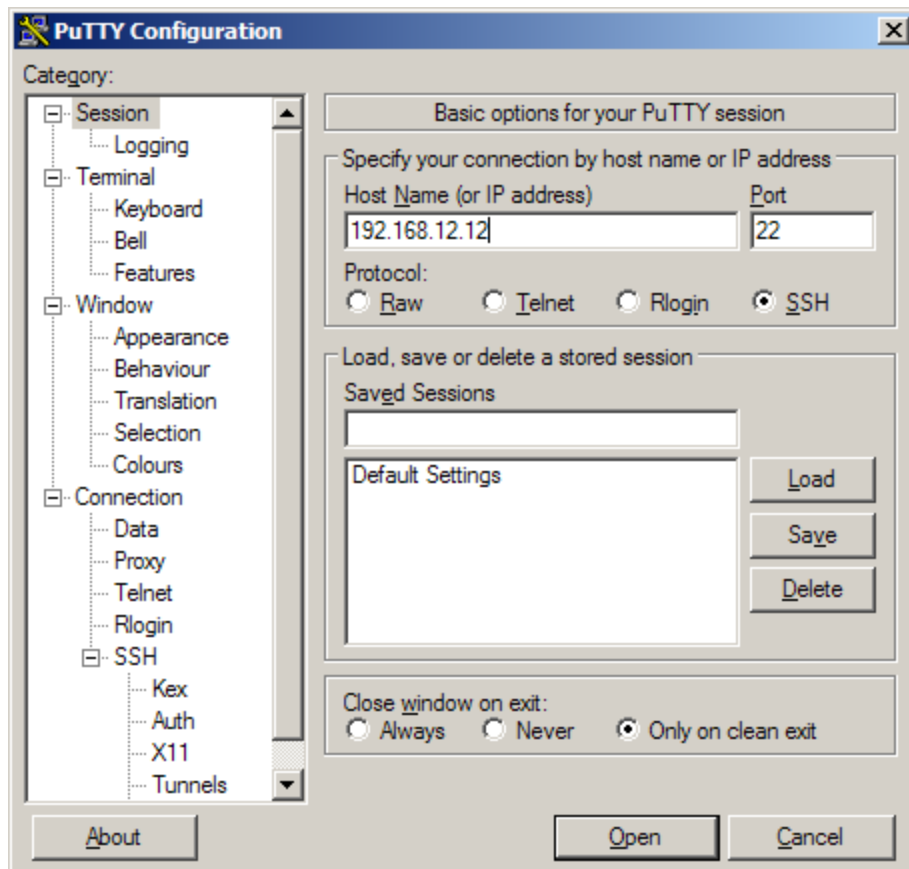
- **On Windows**

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 or CUCM using the PuTTY application, follow these steps:

Note: The following steps are for extracting the host key using the PuTTY application, but you can use any other similar application.

1. Open the PuTTY application and type the host name or IP address of the CM or CUCM under 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.

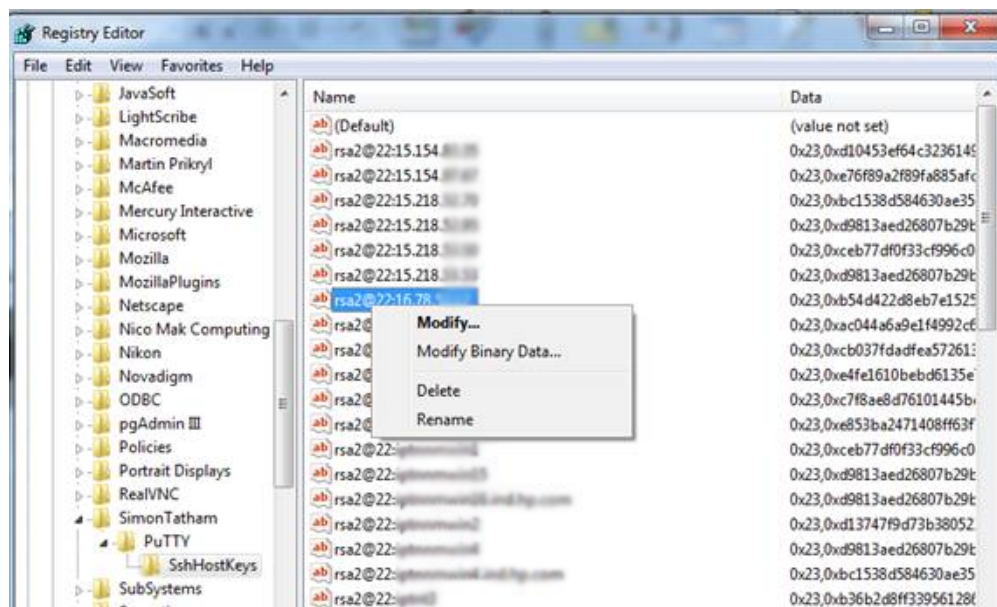
Note: If the pop-up window does not open, go to [step 5](#).

5. If the pop-up window mentioned in [step 4](#) does not open, the host key for the IP address of the CM or CUCM is already cached in the registry by PuTTY in a previous session. In this scenario, you must clear the registry entry and perform [step 1](#) to [step 4](#) again.

To clear the registry entry:

- 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 or CUCM.
 - c. Click **Delete**.
6. Repeat [step 1](#) to [step 4](#).

CDR Access Configuration

Specify the following details on the CDR Access Configuration page:

- **Physical Server IP:** Specifies the IP address of the communication manager server. The This field is populated by default.
- **CDR Format:** Specifies the Call Details Record (CDR) format on the communication manager server. This field is populated by default.
- **Circuit ID Modified:** **True** value specifies 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

This field is populated by default.

- **Date Format:** Specifies the format of the date strings in the CDR records according to the configuration that you specified for the date format in the communication manager server configuration. **DD** specifies the date and **MM** specifies the numeric month. This field is populated by default.
- **Format Specification File Path:** Specifies the absolute path of the customized CDR format specification file on the NNM iSPI for IP Telephony server if the format of the CDR is customized. This field is populated by default.
- **TimeZone:** Type the time zone of the communication manager server in GMT+/- HH:MM format.
- **Configured for Survivability:** **True** value specifies that the data access configuration is configured for survivable CDRs on the communication manager. This field is populated by default.

You must specify the following SFTP details if you select **True** for this option:

- **SFTP Username:** Type the Secure File Transfer Protocol (SFTP) user name to be used by the NNM iSPI for IP Telephony to access or download the CDR files from the communication manager server.
- **SFTP Password:** Type the password for the SFTP user name specified.

You must specify the following details if you select **False** for this option:

- **CDR Port Number:** Type the CDR port number on the NNM iSPI for IP Telephony server.
- **RSP Connectivity Timer:** Type the RSP Connectivity Timer value configured on the Avaya Communication Manager.
- **RSP Packet Response Timer:** Type the RSP Packet Response Timer value configured on the Avaya Communication Manager.

- **Is CDR data sent through a CLAN or Processor Ethernet?:** Select **Yes** to enable this option. This field is populated by default.
You must specify the following information if you enable this option:

IP Address of remote IP Node: Type the IP address for the CLAN or the Processor Ethernet through which the data is sent.

Click **Next**. The [RTCP Configuration](#) page opens.

Note: If the CDR configuration parameters are not auto-populated in the Quick Start Wizard, you must enter the details manually. For more information, see [Obtaining CDR Configuration Parameters from the Avaya Communication Manager](#).

Obtaining CDR Configuration Parameters from the Avaya Communication Manager

To obtain the CDR configuration parameters from the Avaya Communication Manager:

Log on to the Avaya Communication Manager and run the following command to determine if the CDR is survivable or non-survivable:

```
display system-parameters cdr
```

- If the `Enable CDR Storage on Disk` parameter is set to `y`, the CDR is survivable.
Click [here](#) to see the steps to obtain the configuration parameters:
 - a. Copy the parameter values from the Avaya Communication Manager to the corresponding Quick Start Wizard fields as listed in the following table:

Avaya Communication Manager Parameters	Quick Start Wizard Fields
Primary Output Format	CDR Format Note: If the value of the <code>Primary Output Format</code> field is customized, you must create a customized file. For more information, see Creating Customized File .
Modified Circuit ID Display	Circuit ID Modified
CDR Date Format	Date Format Note: Select <code>MMDD</code> for month/day and <code>DDMM</code> for day/month.

File View Help

Command:

F1 F2 F3 F4 F5 F6 F7 F8

display system-parameters cdr Page 1 of 2

CDR SYSTEM PARAMETERS

Node Number (Local PBX ID): 1 CDR Date Format: month/day

Primary Output Format: customized Primary Output Endpoint: DISK

Use ISDN Layouts? n Enable CDR Storage on Disk? y

Use Enhanced Formats? n Condition Code 'T' For Redirected Calls? n

Use Legacy CDR Formats? n Remove # From Called Number? n

Modified Circuit ID Display? n

Record Outgoing Calls Only? n Outg Trk Call Splitting? y

Suppress CDR for Ineffective Call Attempts? n Outg Attd Call Record? y

Disconnect Information in Place of FRL? n Interworking Feat-flag? n

Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n

Calls to Hunt Group - Record: member-ext

Record Called Vector Directory Number Instead of Group or Member? n

Record Agent ID on Incoming? n Record Agent ID on Outgoing? n

Inc Trk Call Splitting? n

Record Non-Call-Assoc TSC? n Call Record Handling Option: warning

Record Call-Assoc TSC? n Digits to Record for Outgoing Calls: dialed

Privacy - Digits to Hide: 0 CDR Account Code Length: 15

Info:

- b. Select the **TimeZone** based on the time zone configuration on the Avaya Communication Manager.
- c. Set the value of the **Configured for Survivability** field to `true`.
- If the **Enable CDR Storage on Disk** parameter is set to `n`, the CDR is non-survivable. Click here to see the steps to obtain the configuration parameters:
 - a. Copy the parameter values from the Avaya Communication Manager to the corresponding Quick Start Wizard fields as listed in the following table.

Avaya Communication Manager Parameters Quick Start Wizard Fields	
Primary Output Format/Secondary Output Format	<p>CDR Format</p> <p>If the NNM iSPI for IP Telephony server is configured as CDR1 endpoint, select the value specified in the Primary Output Format field.</p> <p>If the NNM iSPI for IP Telephony server is configured as CDR2 endpoint, select the value specified in the Secondary Output Format field.</p>

Avaya Communication Manager Parameters Quick Start Wizard Fields	
	Note: If the value of the Primary Output Format field is customized, you must create a customized file. For more information, see Creating Customized File .
Modified Circuit ID Display	Circuit ID Modified
CDR Date Format	Date Format Select MMDD for month/day and DDMM for day/month.

File View Help

Command: Send

CANCEL REFRESH HELP NEXT PA... PREV PA...

F1 F2 F3 F4 F5 F6 F7 F8

display system-parameters cdr Page 1 of 2

CDR SYSTEM PARAMETERS

Node Number (Local PBX ID): 1	CDR Date Format: month/day
Primary Output Format: customized	Primary Output Endpoint: CDR1
Secondary Output Format: customized	Secondary Output Endpoint: CDR2

Use ISDN Layouts? n Enable CDR Storage on Disk? n

Use Enhanced Formats? n Condition Code 'T' For Redirected Calls? n

Use Legacy CDR Formats? n Remove # From Called Number? n

Modified Circuit ID Display? n Intra-switch CDR? y

Record Outgoing Calls Only? n Outg Trk Call Splitting? y

Suppress CDR for Ineffective Call Attempts? y Outg Attd Call Record? y

Disconnect Information in Place of FRL? n Interworking Feat-flag? n

Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n

Calls to Hunt Group - Record: member-ext

Record Called Vector Directory Number Instead of Group or Member? n

Record Agent ID on Incoming? n Record Agent ID on Outgoing? n

Inc Trk Call Splitting? n

Record Non-Call-Assoc TSC? n Call Record Handling Option: warning

Record Call-Assoc TSC? n Digits to Record for Outgoing Calls: dialed

Privacy - Digits to Hide: 0 CDR Account Code Length: 15

Info:

- Select the **TimeZone** based on the time zone configuration on the Avaya Communication Manager.
- Set the value of the **Configured for Survivability** field to false.
- Type the **CDR Port Number**. To find the CDR port number, run the following command:
display ip-services

Select remote port of CDR1 or CDR2 based on whether the NNM iSPI for IP Telephony server is configured as CDR1 or CDR2.

The screenshot shows a terminal window with a menu bar (File, View, Help) and a command input field containing 'display ip-services'. Below the command field are buttons for CANCEL, REFRESH, HELP, NEXT PA..., and PREV PA..., along with function keys F1 through F8. The output of the command is displayed in a table format, showing IP SERVICES configuration for CDR1 and CDR2. The table has columns for Service Type, Enabled, Local Node, Local Port, Remote Node, and Remote Port. The data for CDR1 and CDR2 is as follows:

Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
CDR1	procr	0	blr-cdr-node1	8787	
CDR2	procr	0	blr-cdr-node2	8787	

The page number 'Page 1 of 3' is displayed in the top right corner of the output area. An 'Info:' field is visible at the bottom of the window.

- e. Type the **RSP Connectivity Timer**. To find the RSP Connectivity Timer, run the following command:

```
display ip-services
```

Select RSP Connectivity Timer of CDR1 or CDR2 based on whether the NNM iSPI for IP Telephony server is configured as CDR1 or CDR2.

File View Help

Command: display ip-services

CANCEL
REFRESH

F1 F2 F3 F4 F5 F6 F7 F8

HELP
NEXT PA...
PREV PA...

Send

display ip-services
Page 3 of 3

SESSION LAYER TIMERS

Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer
CDR1	y	30	3	3	60
CDR2	n	30	3	3	60

Info:

- f. Type the **RSP Packet Response Timer**. To find the RSP Packet Response Timer, run the following command:
display ip-services

Select RSP Packet Response Timer of CDR1 or CDR2 based on whether the NNM iSPI for IP Telephony server is configured as CDR1 or CDR2.

File View Help

Command:

F1 F2 F3 F4 F5 F6 F7 F8

display ip-services Page 3 of 3

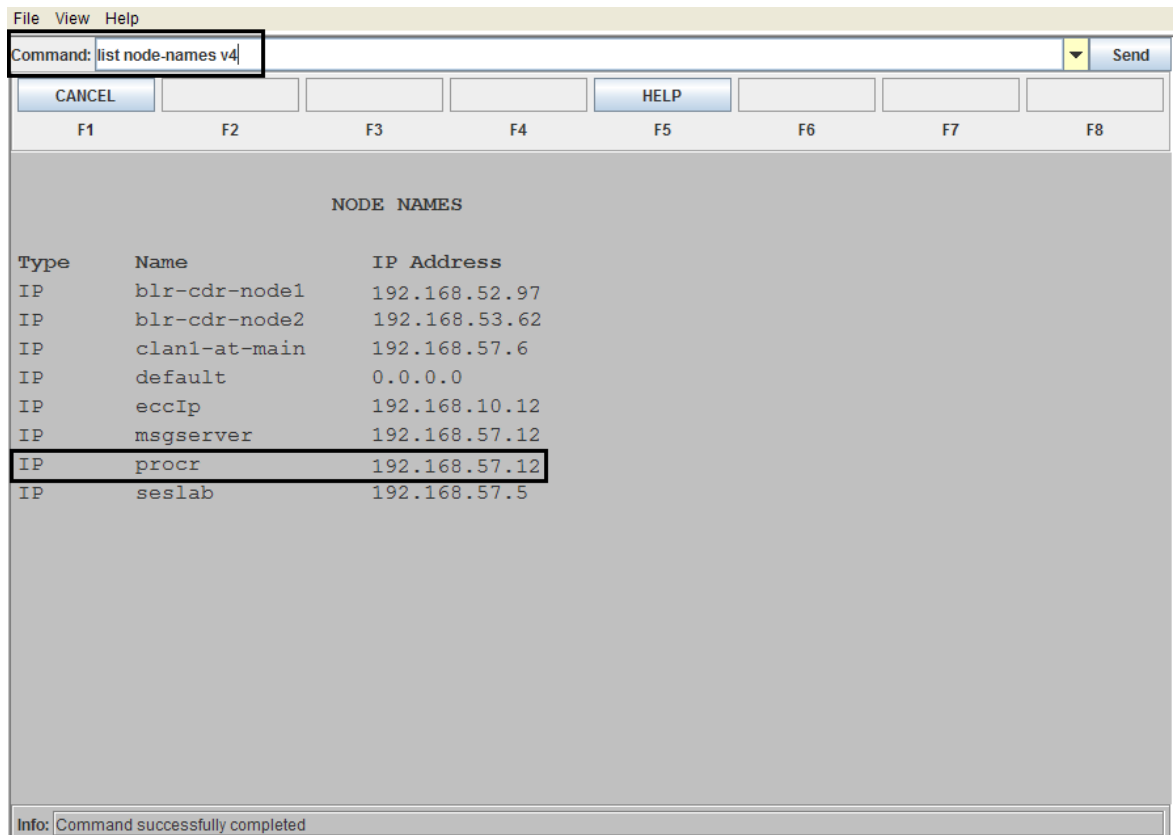
SESSION LAYER TIMERS						
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	
CDR1	y	30	3	3	60	
CDR2	n	30	3	3	60	

Info:

- g. Select the value for **Is CDR data sent through a CLAN or Processor Ethernet** field. To verify if the CDR data is sent through a CLAN or Processor Ethernet configured on Avaya Communication Manager, run the following command:
- ```
display ip-services
```

If the value of the **Local Node** field is `procr`, the CDR data is sent through a processor Ethernet.

- h. Type the IP Address in **IP Address of remote IP Node** field. To find the IP Address of the remote node, run the following command:
- ```
list node-names v4
```

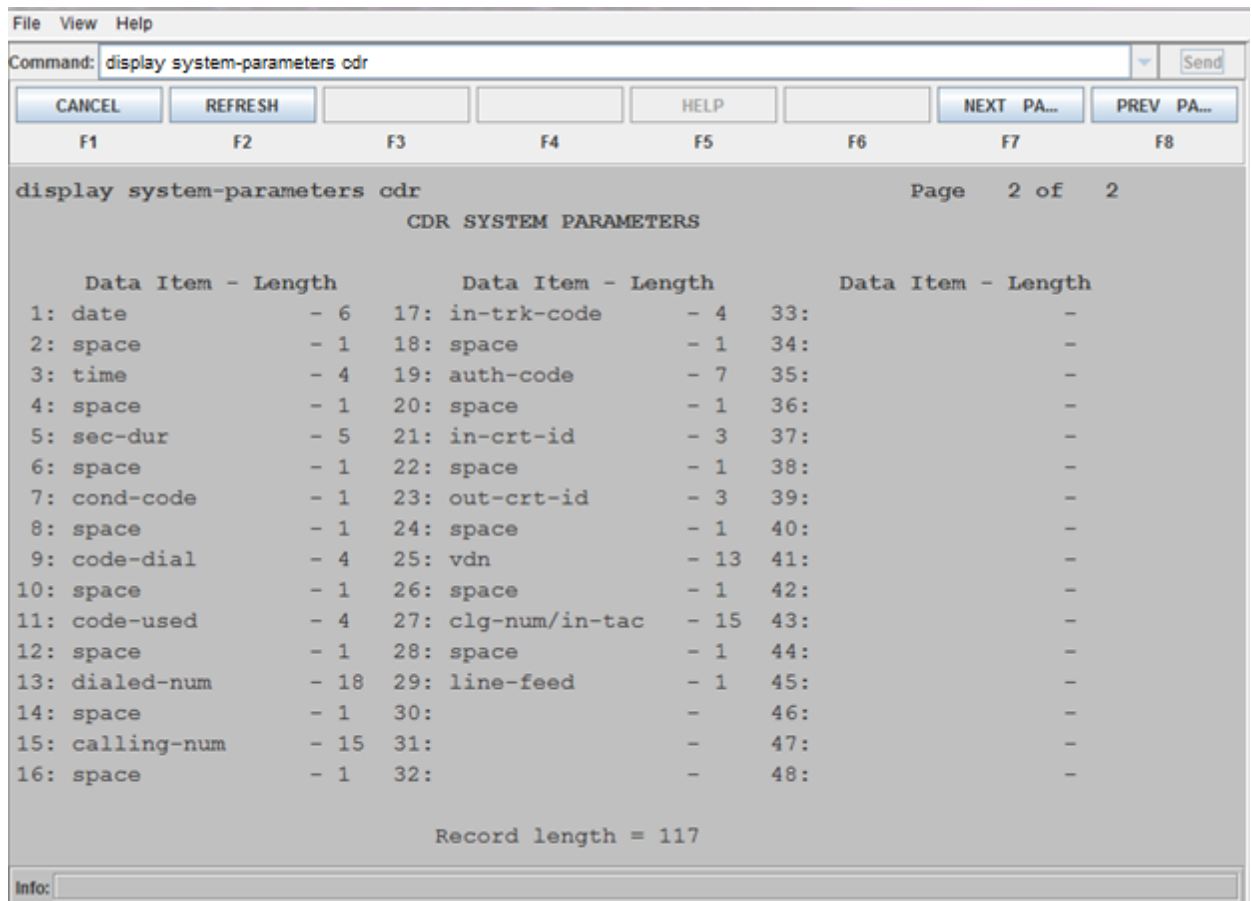


Creating a Customized File

To create a customized file:

1. Log on to the NNMi management server.
2. Navigate to the following directory:
On Windows:
`%nnmdatadir%\shared\ipt\conf`
On UNIX/Linux:
`/var/opt/OV/shared/ipt/conf`
3. Open the `CustomizedCDRFormat.properties` file with a text editor.
`CustomizedCDRFormat.properties` is the sample customized CDR format specification file provided by the NNM iSPI for IP Telephony.
4. Modify the `CustomizedCDRFormat.properties` file to specify the Avaya CDR format based on your requirements.
5. Save and close the `CustomizedCDRFormat.properties` file.

Sample Customized CDR Format Specifications:



```
# 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
time=6-9
sec-dur=10-14
cond-code=15-16
```

```
code-dial=17-20
code-used=21-24
dialed-num=25-42
calling-num=43-57
in-trk-code=58-61
auth-code=62-68
in-crt-id=69-71
out-crt-id=72-74
vdn=75-87
clg-num/in-tac=88-102
line-feed=103-104
```

RTCP Configuration

Specify the following details on the RTCP Configuration page:

- **IP address on the NNM iSPI for IP Telephony:** Enter 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 this communication manager.
- **Type of IP address on the NNM iSPI for IP Telephony system:** Specifies the IP address type for the NNM iSPI for IP Telephony server. This field is populated by default. Only IPv4 addresses are currently supported.
- **UDP Port on the NNM iSPI for IP Telephony system:** Enter 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 this communication manager.
- **IP Address of the Communication Manager:** IP Address of the Communication Manager whose RTP end-points are configured to send RTCP packets to the NNM iSPI for IP Telephony server.
- **Type of IP address of the Communication Manager:** Specifies the remote IP address type of the Communications Manager. This field is populated by default. Only IPv4 addresses are currently supported.
- **Tenant:** Specify the name of the tenant.

Click **Next**. The [Summary](#) page opens.

Note: If the RTCP reception configuration parameters are not auto-populated in the Quick Start Wizard, you must enter the details manually. For more information, see [Obtaining RTCP Configuration Parameters from the Avaya Communication Manager](#).

Obtaining RTCP Configuration Parameters from the Avaya Communication Manager

To obtain the RTCP configuration parameters from the Avaya Communication Manager:

1. Log on to the Avaya Communication Manager and run the following command:

```
display system-parameters ip-options
```

2. Copy the parameter values from the Avaya Communication Manager to the corresponding Quick Start Wizard fields as listed in the following table:

Avaya Communication Manager Parameters	Quick Start Wizard Fields
Server IPv4 Address	IP address on iSPI for IP Telephony system Note: Make sure that the IPv4 address points to the NNM iSPI for IP Telephony server.
IPv4 Server Port	UDP Port on iSPI for IP Telephony system

File View Help

Command:

F1 F2 F3 F4 F5 F6 F7 F8

display system-parameters ip-options Page 1 of 3

IP-OPTIONS SYSTEM PARAMETERS

IP MEDIA PACKET PERFORMANCE THRESHOLDS

Roundtrip Propagation Delay (ms) High: 800 Low: 400

Packet Loss (%) High: 40 Low: 15

Ping Test Interval (sec): 20

Number of Pings Per Measurement Interval: 10

Enable Voice/Network Stats? n

RTCP MONITOR SERVER

Server IPv4 Address: 192.168.53.70 RTCP Report Period(secs): 5

IPv4 Server Port: 10200

Server IPV6 Address:

IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON

Link Failure? y

H.323 IP ENDPOINT

H.248 MEDIA GATEWAY

Link Loss Delay Timer (min): 5

Primary Search Time (sec): 75

Periodic Registration Timer (min): 20

Short/Prefixed Registration Allowed? y

Info:

Summary

Summary page displays the summarized information that you provided in various pages on the NNM iSPI for IP Telephony Quick Start Wizard for Avaya. You can review the information displayed on this page.

Click **Commit** to save and apply the changes.

Click **Previous** to go to the [RTCP Configuration](#) page.

Click **Start Over** to clear the entries in the NNM iSPI for IP Telephony Quick Start Wizard for Avaya and re-enter all the details.

NNM iSPI for IP Telephony Quick Start Wizard for Cisco

You can use the NNM iSPI for IP Telephony Quick Start Wizard for Cisco to configure the NNM iSPI for IP Telephony to access management data from the Cisco IP Telephony servers in your environment.

UCM Publisher

Specify the following details on the UCM Publisher page:

- **Cluster ID:** Type the cluster identifier.
- **Tenant Name:** Select the name of the tenant.
- **Publisher Management IP Address:** Type the IP address of the publisher CM node in your cluster.

Click **Next**. The [AXL Configuration](#) page opens.

AXL Configuration

Specify the following details on the AXL Configuration page:

- **Cluster ID:** Specifies the cluster identifier. This field is populated by default.
- **Tenant Name:** Specifies the name of the tenant. This field is populated by default.
- **Publisher Management IP Address:** Specifies the IP address of the publisher CM node in your cluster. This field is populated by default.
- **AXL Username:** Type the AXL user name to be used for invoking the AXL Web Services.
- **AXL Password:** Type the password associated with the user name specified.

Click **Test** to test the configurations on this page.

Click **Next**. The [SNMP Configuration](#) page opens.

SNMP Configuration

Specify the following details on the SNMP Configuration page:

- **UCM Name:** Specifies the hostname of the UCM. This field is populated by default.
- **IP Address/Host Name:** Specifies the IP address of the UCM. This field is populated by default.
- **Management IP:** Type the IP address of each call manager.
- **SNMP Community String:** Type the SNMP community string for the each call manager.

Click **Previous** to go back to the [AXL Configuration](#) page.

Click **Next** to go to the [SSH Configuration](#) page.

Click **Test** to test the configurations on the SNMP Configuration page.

SSH Configuration

Specify the following details on the SSH Configuration page:

- **UCM Name:** Specifies the hostname of the UCM. This field is populated by default.
- **Management IP:** Specifies the IP address of each call manager. This field is populated by default.
- **Username:** Type the user name to be used to establish an SSH connection.
- **Password:** Type the password to be used for the user name.
- **Host Key:** Type the SSH host key for the call manager. For details on extracting host key, see [Extracting a Host Key for the Avaya Communication Manager and Cisco Unified Communication Manager](#).
- **Port:** Specifies the port number to be used for the SSH connection. This field is populated by default.
- **Timeout in secs:** Specify the number of seconds to wait while attempting to run a command before canceling the attempt. This field is populated by default.

Click **Previous** to go to the [SNMP Configuration](#) page.

Click **Next** to go to the [CDR Access Configuration](#) page.

Click **Test** to test the configurations on the SSH Configuration page.

Extracting a Host Key for the Avaya Communication Manager and Cisco Unified Communications Manager

To extract an RSA level 2 host key for Avaya Communication Manager (CM) or Cisco Unified Communications Manager (CUCM), follow these steps:

• On UNIX/Linux

1. Make sure that no trusted host key is stored for the CM or CUCM 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.

- b. Delete the entry that corresponds to the IP address of the CM or CUCM. For example, if the IP address of your CM or CUCM is 192.168.16.17, the host key that corresponds to the CM or CUCM may look like this:

```
192.168.16.17 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEARC1tF99fLtDQxAPoG+JLGnT10WWEtInB2w4SL3+Om6je9deYr8k
```

2. Run an `ssh` command to the IP address of the remote CM or CUCM 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
established.
```

```
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.

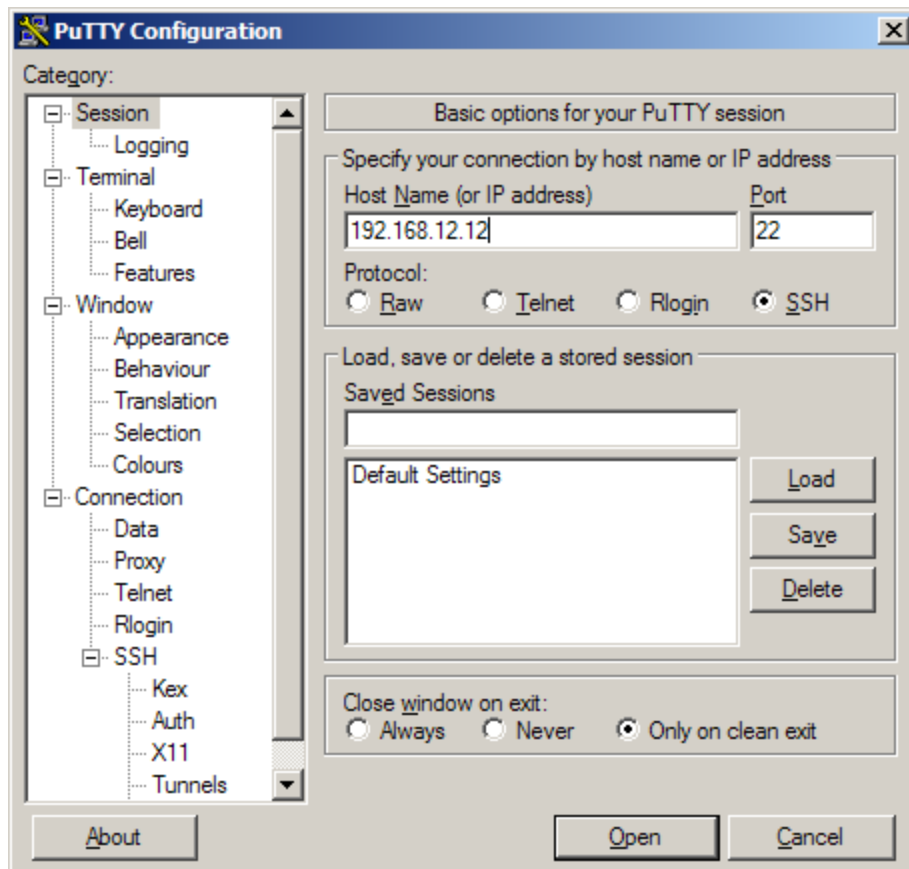
• On Windows

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 or CUCM using the PuTTY application, follow these steps:

Note: The following steps are for extracting the host key using the PuTTY application, but you can use any other similar application.

1. Open the PuTTY application and type the host name or IP address of the CM or CUCM under 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.

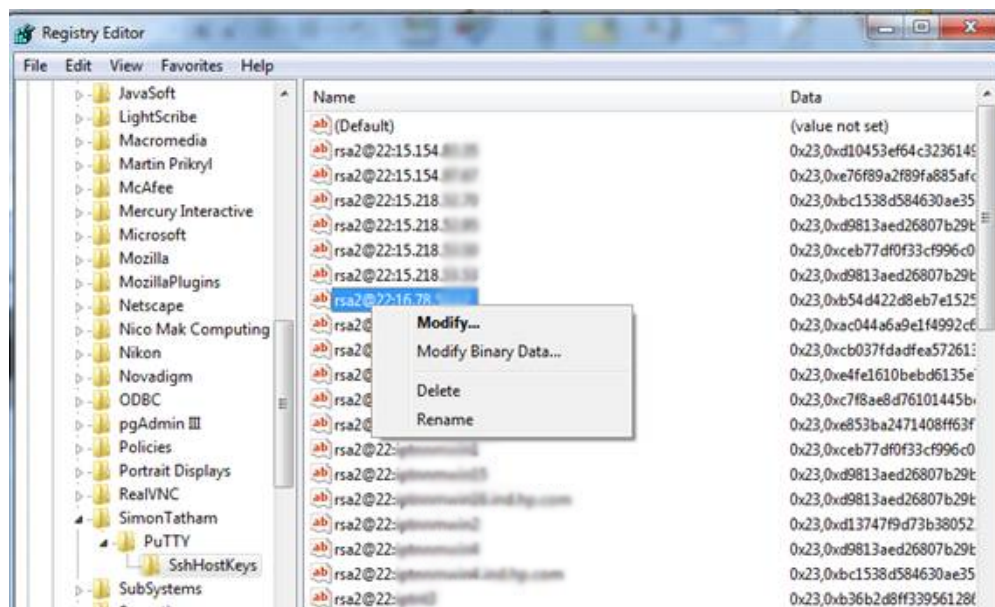
Note: If the pop-up window does not open, go to [step 5](#).

5. If the pop-up window mentioned in [step 4](#) does not open, the host key for the IP address of the CM or CUCM is already cached in the registry by PuTTY in a previous session. In this scenario, you must clear the registry entry and perform [step 1](#) to [step 4](#) again.

To clear the registry entry:

- 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 or CUCM.
 - c. Click **Delete**.
6. Repeat [step 1](#) to [step 4](#).

CDR Access Configuration

Specify the following details on the CDR Access Configuration page:

- **Tenant:** Specifies the name of the tenant. This field is populated by default.
- **Cluster ID:** Specifies the cluster identifier. This field is populated by default.
- **CDR Polling Interval:** Type 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. You can set this interval in the range of 2 minutes to 60 minutes.
- **Is CDR onDemand WS Based Collection?:** 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:** Type the IP address of the Cisco CDR Repository server
 - **SOAP Username:** Type the SOAP user name for the CDRonDemand WebService
 - **SOAP Password:** Type the SOAP password for the CDRonDemand WebService user
 - **Port:** Type the port number for the CDRonDemand WebService port
 - **FTP Username:** Type the FTP user name with write privileges on the NNM iSPI for IP Telephony server.
 - **FTP Password:** Type the password for the FTP user name specified.
 - **Use FTP server FQDN instead of IP Address?:** Select True if you want the NNM iSPI for IP Telephony to use the FTP server FQDN. Select False if the CDR repository nodes are not able to connect to the NNM iSPI for IP Telephony server using the FQDN.
If you select **True**, the FQDN is read from the NNM iSPI for IP Telephony configuration automatically.

If you select **False**, specify the following details:

- **Server FQDN:** Type the FQDN of the NNM iSPI for IP Telephony server
- **Server IP Address:** Type one of the IP Addresses of the NNM iSPI for IP Telephony server. Make sure that the CDR repository nodes in CUCM clusters are able to connect to this server.
- **Application Failover:** Select True if you have Application Failover setup for NNMi and the NNM iSPI for IP Telephony.
 - **Second Server FQDN:** Type the FQDN of the second NNM iSPI for IP Telephony server in Application Failover setup
 - **Second Server IP Address:** Type one of the IP Addresses of the second NNM iSPI for IP Telephony server. Make sure that the CDR repository nodes in CUCM clusters are able to connect to this server.

If you select **False**, specify the complete path to the newly created directory in the **CDR Files Download Path** field. Cisco Unified Communication Manager deems the NNMi management server as a billing server and exports the CDR data to the path specified in the CDR Files Download Path box.

Click **Previous** to go to the [SSH Configuration](#) page.

Click **Next** to go to the [Summary](#) page.

Click **Test** to test the configurations on the CDR Access Configuration page.

Click **Reload** to clear the entries on the CDR Access Configuration page and re-enter all the details.

Summary

Summary page displays the summarized information that you provided in various pages on the NNM iSPI for IP Telephony Quick Start Wizard for Cisco. You can review the information displayed on this page.

Click **Commit** to save and apply the changes.

Click **Previous** to go to the [CDR Access Configuration](#) page.

Click **Start Over** to clear the entries in the NNM iSPI for IP Telephony Quick Start Wizard for Cisco and re-enter all the details.

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 iSPI for IP Telephony. You can access the views to monitor the status and necessary details for every IP Telephony device.

Types of views provided by the iSPI for IP Telephony

View	Purpose
Cisco UCM Clusters	View the discovered Cisco Unified Communications Manager (UCM) clusters available on the network.
Cisco UCMEs	View the discovered Cisco Unified Call Manager Expresses (UCMEs) available on the network.
Cisco IP Phones	View the discovered Cisco IP phones available on the network.
Cisco Gatekeepers	View the discovered Cisco gatekeeper devices available on the network.
Cisco Voice Gateways	View the discovered Cisco voice gateway devices available on the network.
Cisco Unity Devices	View the discovered Cisco Unity devices available on the network.
Avaya Call Controllers	View the discovered Avaya call controllers available on the network.
Avaya IP Phones	View the discovered Avaya IP Phones available on the network.
Avaya Media Gateways	View the discovered Avaya media gateways available on the network.
Nortel Call	View the discovered Nortel Call Servers available on the network.

View	Purpose
Servers	
Nortel Signaling Servers	View the discovered Nortel Signaling Servers available on the network.
Nortel IP Phones	View the discovered Nortel IP phones available on the network.
Nortel Media Gateways	View the discovered Nortel media gateway devices available on the network.

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

IP Telephony Inventory

The iSPI for IP Telephony adds three new workspaces to the NNMi console—the **Cisco IP Telephony**, the **Nortel IP Telephony**, and the **Avaya IP Telephony** workspaces. You can access all the IP Telephony related views from these workspaces. The individual views present device details in tables, and you can launch forms from the views to access the connectivity details.

To launch an IP telephony view:

1. From the Workspaces pane, click **Cisco IP Telephony**, **Nortel IP Telephony**, or **Avaya IP Telephony**. The 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.

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:

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 <i>Not Set</i> 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:

Attribute	Description
	<ul style="list-style-type: none">• 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:

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 IC Trunks: The number of IC trunks associated with the selected UCM cluster.
- Number of Media Devices: The number of media devices associated with the selected UCM cluster.
- Custom Info: The custom information configured for the UCM cluster.

UCM Call Activity tab

This tab provides the count of the types of call activity on the cluster:

- Calls in Progress
- Completed Calls
- Incomplete Calls
- Attempted Calls
- Attempted System Calls
- Active Calls

Configurations tab

This tab provides the count of the route lists and hunt lists in the cluster:

Note: You may not be able to see the counts of the route lists and hunt lists if you have not enabled monitoring of the route lists and hunt lists. For more information, see [Configure Route List and Hunt List Count Monitoring](#).

Registered Devices Count tab

This tab provides the count of the following registered devices in the cluster:

- 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

¹The 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.

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](#).

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:


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  (Save) 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](#)
- [IC Trunks](#)
- [Voice Mail Devices](#)
- [Media Devices](#)


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:

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 <i>Not Set</i> 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](#).


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

¹The 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.

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:

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	<p>The state of the CallManager Service running in the UCM. The possible values are:</p> <ul style="list-style-type: none"> • Up • Down

Attribute	Description
	<ul style="list-style-type: none"> 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	<p>The roles of the UCM. The possible values are as follows:</p> <ul style="list-style-type: none"> 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. <p>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.</p>

You can view the details of a single UCM in a form.

To view the Call Controller form:

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 [Configure 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 [Configure Cisco TFTP Server Monitoring](#).

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 [Configure Registered Devices Count Monitoring](#).

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 [Configure Monitoring of 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 [Select System Health Parameters for Monitoring](#).

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 [Enable Call Activity Monitoring](#).

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	<p>The management status of the node. The status can be any of the following strings:</p> <ul style="list-style-type: none"> • Managed: indicates that the node is managed by the iSPI for IP Telephony. • Out of Service: indicates that the node is currently out of service and not managed by the iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the iSPI for IP Telephony.
Type	<p>The type of the Cisco Call Controller. The type can be one of the following:</p> <ul style="list-style-type: none"> • 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	<p>The CallManager Service State of the selected Cisco Call Controller server. This attribute is not applicable for UCMs.</p> <p>The possible values for a UCM are:</p> <ul style="list-style-type: none"> • 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 the SRST Router. The possible values for an SRST Router state can be one of the following:

Attribute	Description
	<ul style="list-style-type: none"> • 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:

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:

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:

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

N-

ote: 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](#).



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:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > UCM Clusters**. The UCM Clusters view opens in the right pane.

¹The 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.

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](#).
- **IC 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 IC 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:

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	<p>The status of the H.323 gateway device. Possible values are:</p> <ul style="list-style-type: none"> • 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	<p>The name of the device pool to which the H.323 gateway is associated.</p> <p>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.</p>
Call Server	The fully-qualified domain name of the UCM device to which the H.323

Attribute	Description
	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 name of the UCM cluster to which the selected H.323 gateway is associated.
- Device Pool: The name of the device pool to which the selected H.323 gateway is associated.
- Call Server: The fully-qualified domain name of the UCM device 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 handled by the gateway. To see these details, you must enable monitoring of gateway call activity. For more information, see [Configure Gateway Call Activity Monitoring](#).

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:

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.
Management Mode	Displays the management state of the gateway. The status can be one of the following strings: <ul style="list-style-type: none"> • Managed: indicates that the node is

Attribute	Description
	<p>managed by the iSPI for IP Telephony.</p> <ul style="list-style-type: none"> • Out of Service: indicates that the node is currently out of service and not managed by the iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the 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

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	<p>Indicates if the MGCP/SCCP gateway is registered with a UCM.</p> <p>The possible values are as follows:</p> <ul style="list-style-type: none"> • Unknown • Registered • Unregistered • Rejected • Partially Registered
Name	The hostname of the MGCP/SCCP gateway.
Type	<p>The type of the MGCP/SCCP gateway. Possible values are:</p> <ul style="list-style-type: none"> • E and M port

Attribute	Description
	<ul style="list-style-type: none"> • 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	<p>The name of the device pool to which the MGCP/SCCP gateway is associated.</p> <p>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.</p>
Usage State	<p>The usage status of the MGCP/SCCP gateway. This state is not applicable for non-DS1 gateways. Possible values are:</p> <ul style="list-style-type: none"> • 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	<p>This field indicates the operational state of the gateway. Possible values are:</p> <ul style="list-style-type: none"> • 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 [Configure Gateway Call Activity Monitoring](#).

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.

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.

Attribute	Description
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.
Usage State	The usage state of the channel. Possible values are: <ul style="list-style-type: none">• 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:


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: <ul style="list-style-type: none"> • 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. <div> <p>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.</p> </div>

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.
Management Mode	<p>The management status of the node. The status can be any of the following strings:</p> <ul style="list-style-type: none"> Managed: indicates that the node is managed by the iSPI for IP Telephony. Out of Service: indicates that the node is currently out of service and not managed by the iSPI for IP Telephony. Unmanaged: indicates that the node is currently not managed by the iSPI for IP Telephony.
Type	<p>The type of the Cisco Call Controller. The type can be one of the following:</p> <ul style="list-style-type: none"> 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	<p>The CallManager Service State of the selected Cisco Call Controller server. This attribute is not applicable for UCMs.</p> <p>The possible values for a UCM are:</p> <ul style="list-style-type: none"> 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	The IP address of the SRST router interface that the E Phones use to communicate during a fallback.

Attribute	Description
IP	
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	<p>The state of the SRST Router. The possible values for an SRST Router state can be one of the following:</p> <ul style="list-style-type: none"> • 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.

Attribute	Description
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 IC Trunks

The IC Trunks view displays the intercluster trunks (IC trunks) associated with a UCM cluster. The view arranges the key attributes of all associated IC trunks in a table.

To launch the Cisco IC Trunks view:

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 IC Trunks tab. The IC 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: <ul style="list-style-type: none"> • Registered • Unregistered • Rejected • Unknown • Not Applicable (for non-gatekeeper-controlled intercluster trunks)
Name	The name of the Cisco intercluster trunk.
UCM Cluster	The name of the UCM cluster to which the intercluster trunk belongs.
UCM	The name of the Cisco Unified Communications Manager with which the intercluster trunk is associated.
Type	The type of the intercluster trunk. This field indicates if the IC trunk is controlled by the gatekeeper or not.
Active Gatekeeper	The IP address of the gatekeeper device that controls the intercluster trunk. If the intercluster 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 intercluster trunk (for non-gatekeeper-controlled intercluster trunk).
Device Pool	The name of the device pool to which the intercluster trunk is associated. <div> <p>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.</p> </div>

The iSPI for IP Telephony retrieves the registration state of only gatekeeper-controlled intercluster trunks. When the state of an intercluster trunk becomes *Rejected* or *Unregistered*, the iSPI for IP Telephony sends an incident to the NNMi incident browser.

Filtering Cisco IC Trunks

You can filter the listed IC trunks in the IC Trunks view based on the following attributes of the IC 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 IC Trunks view:

1. Right-click any of the listed attribute columns of one of the IC trunks listed in the IC Trunks view.
2. Select one of the following filters:
 - **Equals this value:** filters and lists all the IC 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 IC trunks for which the selected column is not empty.
 - **Is empty:** filters and lists all the IC trunks for which the selected column is empty.
 - **Not equal to this value:** filters and lists all the IC trunks that do not have the value in the column that you selected.

The filtered list of IC trunks appears in the view.

You can also filter the IC 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 intercluster trunk within a form.

To view the H323 Trunk form:

In the IC 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 IC trunk.

Analysis Pane

The Analysis pane provides a summary of the details of a selected intercluster trunk as follows:

H323 Trunk Details Summary tab

- Name: The name of the selected the intercluster trunk.
- Cluster: The name of the UCM cluster to which the selected the intercluster trunk is associated.
- Device Pool: The name of the device pool to which the selected the intercluster trunk is associated.
- Management Server: The management server for the intercluster trunk. This attribute displays one of the following values:
 - Local: If the intercluster trunk is being managed by the NNMI management server console on which you are viewing the intercluster trunk details.
 - Name of the regional manager that manages the intercluster trunk.

ICT Information tab

- Type: The type of the intercluster trunk. This field indicates if the IC 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 intercluster trunk.
- Remote CM List: The list of UCMs that are connected to the intercluster trunk (for non-gatekeeper-controlled intercluster trunk).

H323 Trunk Details Form

The H323 Trunk form helps you view the node details of the selected IC 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 IC trunk.

The left pane lists the following details of the selected Cisco intercluster trunk:

Basic Attributes of the Selected Cisco IC Trunk

Attribute	Description
Name	The name of the intercluster trunk.
Type	Type of the Cisco intercluster trunk.
Remote CM List	The list of Cisco CallManager servers that are connected to the intercluster trunk.
UCM Cluster	The name of the UCM cluster to which the intercluster trunk belongs.

Basic Attributes of the Gatekeeper

Attribute	Description
Configured	The IP address of the gatekeeper device that controls the intercluster trunk.
Alternate	Lists the alternate gatekeeper devices configured to control the intercluster 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 IC Trunks](#).


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:

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	<div>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.</div>

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:

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:

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 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:


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	<p>The management server for the UCME. This attribute displays one of the following values:</p> <ul style="list-style-type: none"> • 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:

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:

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	<p>The management status of the node. The status can be any of the following strings:</p> <ul style="list-style-type: none"> Managed: indicates that the node is managed by the iSPI for IP Telephony. Out of Service: indicates that the node is currently out of service and not managed by the iSPI for IP Telephony. Unmanaged: indicates that the node is currently not managed by the iSPI for IP Telephony.
Type	<p>The type of the Cisco Call Controller. The type can be one of the following:</p> <ul style="list-style-type: none"> 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	<p>The CallManager Service State of the selected Cisco Call Controller server. This attribute is not applicable for UCMs.</p> <p>The possible values for a UCM are:</p> <ul style="list-style-type: none"> 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	The IP address of the SRST router interface that the E Phones use to communicate during a fallback.

Attribute	Description
IP	
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	<p>The state of the SRST Router. The possible values for an SRST Router state can be one of the following:</p> <ul style="list-style-type: none"> • 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.

Attribute	Description
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:

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 with its current controller. Possible values can be as follows: <ul style="list-style-type: none"> • Registered • Unregistered • Unknown • Rejected • Partially Registered
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

Attribute	Description
	for the IP phone.
Management Server	<p>The management server for the IP phone. This attribute displays one of the following values:</p> <ul style="list-style-type: none"> • 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 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 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.
- 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**, **Extension Number**, **IP Address**, **Tenant Controller**, **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:

1. Right-click the **Registration State**, **Extension Number**, **IP Address**, **Tenant Controller**, **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.
Extension Number	The extension number configured for the IP Phone.
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	<p>The management status of the node. The status can be any of the following strings:</p> <ul style="list-style-type: none"> • Managed: indicates that the node is managed by the iSPI for IP Telephony. • Out of Service: indicates that the node is currently out of service and not managed by the iSPI for IP Telephony. • Unmanaged: indicates that the node is currently not managed by the 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.
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.

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:

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 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 UNIX/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:

From the **Workspaces** navigation pane, click > **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.

Attribute	Description
Tenant	The name of the tenant to which the gatekeeper belongs.
H323Endpoints	The number of endpoints associated with the gatekeeper.
Management Server	<p>The management server for the gatekeeper. This attribute displays one of the following values:</p> <ul style="list-style-type: none"> • 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:

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:

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: <ul style="list-style-type: none"> • Managed: indicates that the node is managed by the iSPI for IP Telephony.

Attribute	Description
	<ul style="list-style-type: none"> Out of Service: indicates that the node is currently out of service and not managed by the iSPI for IP Telephony. Unmanaged: indicates that the node is currently not managed by the iSPI for IP Telephony.

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:


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	<p>The management server for the Cisco Unity Device. This attribute displays one of the following values:</p> <ul style="list-style-type: none"> 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:

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.

Attribute	Description
Version	Indicates the version of the device.
Management Mode	<p>Indicates the management state of the device. The state can be one of the following:</p> <ul style="list-style-type: none">• Managed: indicates that the device is managed by the iSPI for IP Telephony.• Out of Service: indicates that the device is currently out of service and not managed by the iSPI for IP Telephony.• Unmanaged: indicates that the device is currently not managed by the 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 Manager clusters, 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 configure thresholds.* Incidents in the incidents inventory

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

If you log on as `operator 1` or `operator 2`, and if Single Sign-On is configured, you can configure additional monitoring attributes for items that you can view in different Cisco IP telephony inventory views that you can access from the UCM Clusters view.

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

Monitor Call Activities

You can configure the NNM iSPI for IP Telephony to monitor call activities for a Cisco Unified Communications Manager or a Cisco Unified Communications Manager cluster. 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.

Enable Call Activity Monitoring

You must perform the following tasks to configure call activity monitoring:


1. Configure SSH credentials for the Cisco Unified Communication Manager you want to monitor. See the section ["Configuring Data Access for Cisco" \(on page 245\)](#) for more details.
2. Enable call activity monitoring.
3. Configure Call Activity Configuration Settings. See ["Select Call Activities for Monitoring" \(on page 99\)](#) for more details.

To enable call activity monitoring:

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. Select a cluster from the UCM Clusters view and 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. Select **UCM Call Activity** from the **Area of Monitoring** drop-down list.
5. 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 call activity for the cluster periodically.
6. Select **Apply Configuration Setting to Other UCM Clusters** option if you want the call activity monitoring settings to be applied on other clusters.
7. Specify the common custom information configured for the other clusters in the box provided.
8. Click  **Save** to save the monitoring configuration.

Note: 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 page for the Cisco Unified Communications Manager. However, you cannot specify the data collection and CSV export intervals if you launch the Monitoring Configuration form for a particular Cisco Unified Communications Manager. You must always specify the collection and export intervals for Cisco Unified Communications Manager clusters. Individual Cisco Unified Communications Managers assume the intervals specified for the corresponding cluster.

The right pane on the Monitoring Configuration for UCM Cluster page displays the list of existing UCM Call Activity configuration settings under the UCM Call Activity tab along with the attributes enabled for each UCM call activity configuration. A tick mark below the attribute indicates that the attribute is enabled for the UCM call activity configuration. See the ["Select Call Activities for Monitoring" \(on page 99\)](#) for more details regarding the attributes listed on this pane.

To add call activity configuration settings, click  (New) from the right pane on the Monitoring Configuration for UCM Cluster page. See the ["Select Call Activities for Monitoring" \(on page 99\)](#) for more details.

To Modify an Existing Call Activity Configuration Setting:

1. Select the call activity configuration that you want to modify and click **Edit**. This opens the Edit Call Activity Configuration Settings page.
2. Make the required changes and click **Save** to save the modified configuration settings.

To Delete an Existing Call Activity Configuration Setting:


Select the call activity configuration that you want to delete and click **Delete**. You can click **Delete All** to delete all the call activity configuration settings.

To Disable an Existing Call Activity Configuration Setting:

Select the call activity configuration that you want to disable and click **Disable**.

Select Call Activities for Monitoring

The UCM Call Activity Configuration page helps you to configure the call activity settings such as specifying threshold settings to generate incidents, enabling monitoring for call activity, and enabling reporting for call activity.

1. Click  (New) from the right pane on the Monitoring Configuration for UCM Cluster page. This opens the UCM Call Activity Configuration page.

Note: Clicking **New** from the right pane on the Monitoring Configuration for UCM page displays the UCM Call Activity Configuration page that you can use to configure call activity settings for a Cisco Unified Communications Manager.


2. Select the call activity to be monitored from the **Measurement Type** drop-down list. You can select one of the following types of call activity:
 - **Calls in Progress**
 - **Completed Calls**
 - **Incomplete Calls**
 - **Attempted Calls**
 - **Attempted System Calls**
 - **Active Calls**
3. Select **Enable Monitoring** to configure the NNM iSPI for IP Telephony to start monitoring the selected call activity.
4. Select **Threshold Check** to specify the threshold settings that you want to configure for the monitored call activity.
5. Select one of the following options from the **Severity** drop-down list to configure the severity of the incident that must be generated during a threshold violation. Based on your selection, the iSPI for IP Telephony generates the incident listed adjacent to the severity level below in parenthesis:
 - **Critical:** (*MonitoredAttributeThresholdBreachCritical*)
 - **Major:** (*MonitoredAttributeThresholdBreachMajor*)
 - **Minor:** (*MonitoredAttributeThresholdBreachMinor*)
 - **Warning:** (*MonitoredAttributeThresholdBreachWarning*)

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 listed.

6. Specify the following values to configure the lower base threshold settings:
 - **Lower Base:** specifies the lower value for the call activity threshold.
 - **%Deviation:** specifies the acceptable percentage of deviation from the lower base threshold value before generating an incident.

- **Abs Lower Deviation:** specifies the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
- **Lower Trigger Count:** specifies the minimum number of times the threshold deviation must be permitted before generating the incident. Specifying the trigger count is mandatory for generating incidents.

Note: You can either specify the **%Deviation** or the **Abs Lower Deviation** value.

7. Specify the following values to configure the higher base threshold settings:
 - **Higher Base:** specifies the higher value for the call activity threshold.
 - **%Deviation:** specifies the acceptable percentage of deviation from the higher base threshold value before generating an incident.
 - **Abs Higher Deviation:** specifies the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
 - **Higher Trigger Count:** specifies the maximum number of times the threshold deviation must be permitted before generating the incident. Specifying the trigger count is mandatory for generating incidents.
8. Click  **Save** to save the call activity configuration settings.

Note: If required, you can specify both the lower base threshold setting and the higher base threshold setting for a call activity configuration.

For example, if you have configured the following call activity settings to monitor call activity based on the Incomplete Calls call activity :

- Lower Base: 110
- %Deviation: 10%
- Higher Trigger Count: 10

In this scenario, the NNM iSPI for IP Telephony generates the threshold violation incident when the following conditions are true:

- The number of incomplete calls reaches below 100 for the cluster.
- The number of times the incomplete calls count reaches below 100 is above 10 for the cluster.

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:

- 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

N-

ote: 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 the NNM iSPI for IP Telephony.

You can configure thresholds for the monitored devices. The NNM iSPI for IP Telephony generates *MonitoredAttributeThresholdBreach* incidents when the thresholds are violated.

Example:

You configured the following registered devices count settings to monitor the count of hardware phones:

- Lower Base: 100
- Higher Base: 1000

In this scenario, the NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreach* incident when one of the following conditions is true:

- The count of hardware phones reaches below 100 for the cluster.
- The count of hardware phones reaches above 1000 for the cluster.

You must perform the following tasks to configure registered device count monitoring:

1. Configure AXL credentials for the cluster that you want to monitor. See ["Configuring Data Access for Cisco" \(on page 245\)](#) for more details.

¹The 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.



2. Configure registered device count monitoring. See ["Enable Registered Devices Count Monitoring" \(on page 102\)](#) for more details.
3. Configure registered device count monitoring configuration settings. See [Configuring Registered Devices Count Settings](#) for more details.

Enable Registered Devices Count Monitoring

To configure the monitoring of registered device count:

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 **Actions > IP Telephony > Monitoring Configuration**. The Monitoring Configuration for UCM Cluster form opens.

Tip: Alternatively, 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. You cannot even enable or disable monitoring. However, you can modify the threshold settings from these forms. You can also enable or disable CSV export.

3. Select **Registered Devices Count** from the **Area of Monitoring** drop-down list. The right pane displays the devices configured for monitoring.
4. Select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The iSPI for IP Telephony uses this value to monitor the counts of the registered devices for the cluster periodically.
5. Select minutes (**mins**) or hours (**hrs**) from the **CSV Export Interval** drop-down list and specify the value in the respective box. The iSPI for IP Telephony uses this value to export the counts of the monitored devices for the cluster periodically.
6. Select **Apply Configuration Setting to Other UCM Clusters** option if you want the registered device count monitoring settings to be applied on other clusters.
7. Click  **New**. This opens the Registered Devices Count Configuration form.
8. Specify the details in the value box for each of the parameters. See the [Configuring Registered Devices Count Settings](#) for more details regarding the parameters.
9. Click  **Save** to save the monitoring configuration.

The right pane on the Monitoring Configuration for UCM Cluster page displays the list of existing registered devices count configuration settings under the **Registered Devices Count** tab along with the attributes enabled for each registered devices count configuration. A tick mark below the attribute indicates that the attribute is enabled for the registered devices count configuration.


To delete a registered device count monitoring configuration:

1. On the Monitoring Configuration for UCM Cluster form, select the check box of the registered device count monitoring configuration that you want to delete.

2. Click  Delete to delete the registered device count monitoring configuration.

Tip: You can delete all registered device count monitoring configurations by clicking **Delete All**. You can disable all registered device count monitoring configurations by clicking **Disable All**.

To modify a registered device count monitoring configuration:


1. On the Monitoring Configuration for UCM Cluster form, select the check box of the registered device count monitoring configuration that you want to modify.
2. Click  Edit. This opens the **Registered Devices Count Configuration** form.
3. Specify the details in the value box for each of the parameters.
4. Click **Save/Save and close**.

Configuring Registered Devices Count Settings

The Registered Devices Count Configuration page helps you to configure the registered devices count monitoring settings based in a cluster. 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.

The monitoring of the count of the devices enables you to configure thresholds for the monitored devices. The NNM iSPI for IP Telephony generates incidents when the thresholds are violated.

To configure the monitoring of registered device count:

1. Click  New. This opens the Registered Devices Count Configuration form.
2. In the Registered Devices Count Configuration form, specify the following details in the value box for each of the following parameters:
 - **Measurement Type:** specify the device to be configured from the drop-down list. The drop-down list displays the following devices:
 - 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
- **Enable Monitoring:** Select Enable Monitoring to configure the iSPI for IP Telephony to start monitoring the count of the registered devices.
 - **Enable Reporting:** You cannot edit this field. You cannot generate reports for the registered devices count.
 - **Enable CSV Export:** Select this check box to export monitored values in a CSV file. If you select this check box, the NNM iSPI for IP Telephony exports the counts of the monitored devices in the specified interval.
 - **Threshold Check:** Select this check box to specify the threshold settings that you want to configure for the count of the registered devices.
 - **Threshold Severity:** Select one of the following options from the Severity drop-down list to configure the severity of the incident that must be generated during a threshold violation. Based on your selection, the iSPI for IP Telephony generates the incident listed adjacent to the severity level below in parenthesis:
 - **Critical:** (*MonitoredAttributeThresholdBreachCritical*)
 - **Major:** (*MonitoredAttributeThresholdBreachMajor*)
 - **Minor:** (*MonitoredAttributeThresholdBreachMinor*)
 - **Warning:** (*MonitoredAttributeThresholdBreachWarning*)

Note: The iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents listed.

- **Lower Base:** Type the lower value for the count of the registered devices threshold.
- **% Lower Deviation:** Type the acceptable percentage of deviation from the lower base threshold value before generating an incident.
- **Abs Lower Deviation:** Type the acceptable absolute value of deviation from the lower base threshold value before generating the incident.
- **Lower Trigger Count:** Type the minimum threshold violation count. The NNM iSPI for IP Telephony generates the incident when the threshold violation occurs consecutively for the value specified in this box. Specifying the trigger count is mandatory for generating incidents.
- **Higher Base:** Type the higher value for the count of the registered devices threshold.

¹The 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.

- **% Higher Deviation:** Type the acceptable percentage of deviation from the higher base threshold value before generating an incident.
- **Abs Higher Deviation:** Type the acceptable absolute value of deviation from the higher base threshold value before generating the incident.
- **Higher Trigger Count:** Type the maximum threshold violation count. The NNM iSPI for IP Telephony generates the incident when the threshold violation occurs consecutively for the value specified in this box. Specifying the trigger count is mandatory for generating incidents.

3. Click **Save**.

If you select the Enable CSV Export check box, 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.

Configure Cisco TFTP Server Monitoring

You can configure the NNM iSPI for IP Telephony to monitor the following activities related to the configuration file builds performed by the Cisco TFTP server. You can monitor these activities for a UCM.

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.

You can specify the threshold deviation to be monitored for TFTP server activity to generate incidents if thresholds are violated. You can also enable reporting based on the TFTP server activity.


You must perform the following tasks to configure Cisco TFTP server monitoring settings:

1. Configure SSH credentials for the Cisco Unified Communication Manager you want to monitor. See the section "[Configuring Data Access for Cisco](#)" (on page 245) for more details.
2. Configure Cisco TFTP server monitoring settings as shown in the following section.
3. Configure Cisco TFTP Activity Configuration Settings. See [Configure Cisco TFTP Server Monitoring Settings](#) for more details.


To configure Cisco TFTP server monitoring:

1. From the NNMi console, click the **Cisco IP Telephony** workspace on the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view
3. Select a cluster and double click the cluster to open the cluster details form.
4. Select a Cisco Unified Communications Manager from the list of Cisco Unified Communications Managers listed under the UCM tab and double click the UCM to open the UCM Details form.
5. Click **Actions > IP Telephony > Monitoring Configuration** from the menu to launch the Monitoring Configuration for UCM page for the UCM.

Note: You can alternatively launch the Monitoring Configuration for UCM Cluster page by right clicking a cluster from the UCM Clusters view and selecting **IP Telephony > Monitoring Configuration**.


6. Select **Cisco TFTP Server** from the **Area of Monitoring** drop-down list.
7. 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.
8. Click  (Save) to save the monitoring configuration.

The right pane on the Monitoring Configuration for UCM Cluster page displays the list of existing Cisco TFTP server activity configuration settings under the Cisco TFTP Server tab along with the attributes enabled for each activity configuration. A tick mark below the attribute indicates that the attribute is enabled for the Cisco TFTP Server activity configuration.

To add Cisco TFTP server activity configuration settings, click  (New) from the right pane on the Monitoring Configuration for UCM Cluster page. See the [Configure Cisco TFTP Server Monitoring Settings](#) section for more details.

Configure Cisco TFTP Server Monitoring Settings

The Cisco TFTP Server Monitoring Configuration page helps you to configure the Cisco TFTP server activity settings such as specifying threshold settings to generate incidents based on the TFTP server activity, enabling monitoring for the TFTP server activity, and enabling reporting for the TFTP server activity.


1. Click  (New) from the right pane on the Monitoring Configuration for UCM page. This opens the UCM TFTP Activity Configuration page.
2. Select the TFTP server activity to be monitored from the **Measurement Type** drop-down list. You can select one of the following types of activity:

- **BuildAbortCount**
 - **BuildCount**
 - **BuildDeviceCount**
 - **BuildDialRuleCount**
 - **BuildSignCount**
 - **BuildSoftKeyCount**
 - **BuildUnitCount**
 - **ChangeNotifications**
 - **DeviceChangeNotifications**
 - **DialRuleChangeNotifications**
 - **HTTPRequestsAborted**
 - **HTTPRequestsProcessed**
 - **RequestsAborted**
 - **RequestsProcessed**
3. Select **Enable Monitoring** to configure the iSPI for IP Telephony to start monitoring the selected TFTP server activity.
 4. Select **Enable Reporting** to configure the iSPI for IP Telephony to start reporting based on the selected TFTP server activity.
 5. Select **Threshold Check** to specify the threshold settings that you want to configure for the monitored TFTP server activity.
 6. Select one of the following options from the **Severity** drop-down list to configure the severity of the incident that must be generated during a threshold violation. Based on your selection, the iSPI for IP Telephony generates the incident listed adjacent to the severity level below in parenthesis:
 - **Critical:** (*MonitoredAttributeThresholdBreachCritical*)
 - **Major:** (*MonitoredAttributeThresholdBreachMajor*)
 - **Minor:** (*MonitoredAttributeThresholdBreachMinor*)
 - **Warning:** (*MonitoredAttributeThresholdBreachWarning*)

Note: The iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents listed.
 7. Specify the following values to configure the lower base threshold settings:
 - **Lower Base:** specifies the lower value for the threshold.
 - **%Deviation:** specifies the acceptable percentage of deviation from the lower base threshold value before generating an incident.

- **Abs Lower Deviation:** specifies the acceptable absolute value of deviation for the lower base threshold value before generating the incident.
- **Lower Trigger Count:** specifies the minimum number of times the threshold deviation must be permitted before generating the incident. Specifying the trigger count is mandatory for generating incidents.

Tip: You can either specify the **%Deviation** or the **Abs Lower Deviation** value.

8. Specify the following values to configure the higher base threshold settings:
 - **Higher Base:** specifies the higher value for the TFTP server activity threshold.
 - **%Deviation:** specifies the acceptable percentage of deviation from the higher base threshold value before generating an incident.
 - **Abs Higher Deviation:** specifies the acceptable absolute value of deviation for the higher base threshold value before generating the incident.
 - **Higher Trigger Count:** specifies the maximum number of times the threshold deviation must be permitted before generating the incident. Specifying the trigger count is mandatory for generating incidents.
9. Click  (Save) to save the TFTP server activity configuration settings.

Note: If required, you can specify both the lower base threshold setting and the higher base threshold setting for a TFTP server activity configuration.

For example, if you have configured the following TFTP server activity settings to monitor TFTP server activity based on the `BuildAbortCount` TFTP server activity :

- Lower Base: 110
- %Deviation: 10%
- Higher Trigger Count: 10

In this scenario, the iSPI for IP Telephony generates the threshold violation incident when the following conditions are true:

- The number of aborted builds reaches below 100 for the UCM.
- The number of times the `BuildAbortCount` reaches below 100 is above 10 for the UCM.

Configure Route List and Hunt List Count Monitoring



You can monitor the count of route and hunt lists based in a cluster. A route list is a set of route groups arranged in a specific order. A route list is responsible for regulating the available devices for outgoing calls. A hunt list is a set of line groups arranged in a specific order. A hunt list is responsible for regulating the available directory numbers for incoming calls.

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.

You must perform the following tasks to configure route list and hunt list count monitoring:


1. Configure AXL credentials for the cluster that you want to monitor. See the section ["Configuring Data Access for Cisco" \(on page 245\)](#) for more details.
2. Configure route list and hunt list count monitoring as shown in the following section.
3. Configure registered device count monitoring configuration settings. See [Configuring Route List and Hunt List Count Settings](#) for more details.

To configure the monitoring of route list or hunt list count:

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 **Actions > IP Telephony > Monitoring Configuration**. The Monitoring Configuration for UCM Cluster form opens.
3. Select **Configurations** from the **Area of Monitoring** drop-down list.
4. Select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The iSPI for IP Telephony uses this value to monitor the counts of the route lists and hunt lists for the cluster periodically.
5. Select minutes (**mins**) or hours (**hrs**) from the **CSV Export Interval** drop-down list and specify the value in the respective box. The iSPI for IP Telephony uses this value to export the counts of the monitored devices for the cluster periodically.
6. Select **Apply Configuration Setting to Other UCM Clusters** option if you want the route list and hunt list monitoring settings to be applied on other clusters.
7. Click  **New**. This opens the Configurations Configuration form.
8. Specify the details in the value box for each of the parameters. See the [Configuring Route List and Hunt List Count Settings](#) for more details regarding the parameters.
9. Click  **Save** to save the monitoring configuration.

The right pane on the Monitoring Configuration for UCM Cluster page displays the list of existing route list and hunt list count configuration settings under the **Configurations** tab along with the attributes enabled for these configurations. A tick mark below the attribute indicates that the attribute is enabled for the configuration.


To delete route list or hunt list count monitoring configuration:

1. On the Monitoring Configuration for UCM Cluster form, select the check box of the route list or hunt list count monitoring configuration that you want to delete.
2. Click  **Delete** to delete the route list or hunt list count monitoring configuration.

Tip: You can delete route list and hunt list count monitoring configurations together by clicking **Delete All**. You can disable all route list and hunt list count monitoring configurations by clicking **Disable All**.

To modify route list or hunt list count monitoring configuration:

1. On the Monitoring Configuration for UCM Cluster form, select the check box of the route list or hunt list count monitoring configuration that you want to modify.


2. Click  Edit. This opens the **Configurations Configuration** form.
3. Specify the details in the value box for each of the parameters.
4. Click **Save/Save and close**.

Configuring Route List and Hunt List Count Settings

The Configurations Configuration page helps you to configure the route lists and hunt lists count monitoring settings based in a cluster.

The monitoring of the count of the route lists and the hunt lists enables you to configure thresholds for these lists. The NNM iSPI for IP Telephony generates incidents when the thresholds are violated.

To configure the monitoring of route and hunt lists count:

1. Click  New. This opens the Add Update Configuration form.
2. In the Add Update Configuration form, specify the following details in the value box for each of the following parameters:
 - **Measurement Type:** specify the list to be configured from the drop-down list. The drop-down list displays the following lists:
 - Route List
 - Hunt List
 - **Enable Monitoring:** Select Enable Monitoring to configure the iSPI for IP Telephony to start monitoring the count of the list.
 - **Enable CSV Export:** Select this check box to export monitored values in a csv file. If you select this check box, the NNM iSPI for IP Telephony exports the counts of the monitored lists in the specified interval.
 - **Threshold Check:** Select this check box to specify the threshold settings that you want to configure for the count of the lists.
 - **Threshold Severity:** Select one of the following options from the Severity drop-down list to configure the severity of the incident that must be generated during a threshold violation. Based on your selection, the iSPI for IP Telephony generates the incident listed adjacent to the severity level below in parenthesis:
 - **Critical:** (*MonitoredAttributeThresholdBreachCritical*)
 - **Major:** (*MonitoredAttributeThresholdBreachMajor*)
 - **Minor:** (*MonitoredAttributeThresholdBreachMinor*)
 - **Warning:** (*MonitoredAttributeThresholdBreachWarning*)

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 listed.

- **Lower Base:** Type the lower value for the count of the route or hunt lists threshold.
- **% Lower Deviation:** Type the acceptable percentage of deviation from the lower base

threshold value before generating an incident.

- **Abs Lower Deviation:** Type the acceptable absolute value of deviation from the lower base threshold value before generating the incident.
- **Lower Trigger Count:** Type the minimum threshold violation count. The NNM iSPI for IP Telephony generates the incident when the threshold violation occurs consecutively for the value specified in this box. Specifying the trigger count is mandatory for generating incidents.
- **Higher Base:** Type the higher value for the count of the route and hunt lists threshold.
- **% Higher Deviation:** Type the acceptable percentage of deviation from the higher base threshold value before generating an incident.
- **Abs Higher Deviation:** Type the acceptable absolute value of deviation from the higher base threshold value before generating the incident.
- **Higher Trigger Count:** Type the maximum threshold violation count. The NNM iSPI for IP Telephony generates the incident when the threshold violation occurs consecutively for the value specified in this box. Specifying the trigger count is mandatory for generating incidents.

3. Click **Save**.

If you select the Enable CSV Export check box, 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\Configurations
- On UNIX/Linux: /var/opt/OV/shared/ipt/CSVExport/Cisco/Configurations

To use the CSV files, you must have sufficient privilege to access the above location.

Configure Media Resource Activity Monitoring

The NNM iSPI for IP Telephony enables you 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.

The NNM iSPI for IP Telephony enables you to monitor the following types of resources in each media device:

- **Active Resources:** The number of resources that are currently in use.
- **Unavailable Resources:** 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:** The number of resources that are available to be used. These resources are not in use at the current time.

Monitoring of the media resources enables you to configure thresholds for the resources in the monitored devices. The NNM iSPI for IP Telephony generates *MonitoredAttributeThresholdBreach* incidents when the thresholds are violated. For example, if you have configured the following thresholds to monitor the active resources in a conference bridge:

- Lower Base: 5
- Higher Base: 10

In this scenario, the NNM iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreach* incident when one of the following conditions is true:

- The number of active connections reaches below 5 for the conference bridge.
- The number of active connections reaches above 10 for the conference bridge.

Note: You cannot configure thresholds for media devices if you launch Monitoring Configuration form for a cluster. You have to set thresholds for each media device separately. Launch Monitoring Configuration form from the details form of the media device to set thresholds for the resources in that particular media device.


You must perform the following tasks to configure media resource activity monitoring:


1. Configure SSH credentials for all the Cisco Unified Communication Managers in the cluster that you want to monitor. See the section ["Configuring Data Access for Cisco" \(on page 245\)](#) for more details.
2. Configure media resource activity monitoring as shown in the following section.
3. Configure media resource activity monitoring configuration settings. See [Configuring Media Resource Activity Monitoring Settings](#) for more details.

To configure the monitoring of media resource activity:

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 **Actions > IP Telephony > Monitoring Configuration**. The Monitoring Configuration for UCM Cluster form opens.


Tip: Alternatively, you can also launch Monitoring Configuration form for a media device from the details form of the media device. You cannot add a new media resource activity monitoring configuration for a particular type of media resource from the details form of the media device if you have not 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 configuration for the cluster.

3. Select **Media Resource Activity** from the **Area of Monitoring** drop-down list. The right pane displays the resources configured for monitoring.
4. 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 media resource activity periodically.
5. Select **Apply Configuration Setting to Other UCM Clusters** option if you want the media resource activity monitoring settings to be applied on other clusters.
6. Click  **New**. This opens the Media Resource Activity Configuration form.

7. Specify the details in the value box for each of the parameters. See the [Configuring Media Resource Activity Monitoring Settings](#) for more details regarding the parameters.
8. Click  Save to save the monitoring configuration.


The right pane on the Monitoring Configuration for UCM Cluster page displays the list of existing media resource activity configuration settings under the **Media Resource Activity** tab along with the attributes enabled for each media resource activity configuration. A tick mark below the attribute indicates that the attribute is enabled for the media resource activity configuration.

To delete a media resource activity monitoring configuration:

1. On the Monitoring Configuration for UCM Cluster form, select the check box of the media resource activity monitoring configuration that you want to delete.
2. Click  Delete to delete the media resource activity monitoring configuration.

Tip: You can delete all media resource activity monitoring configurations by clicking **Delete All**. You can disable all media resource activity monitoring configurations by clicking **Disable All**.


To modify a media resource activity monitoring configuration:

1. On the Monitoring Configuration for UCM Cluster form, select the check box of the media resource activity monitoring configuration that you want to modify.
2. Click  Edit. This opens the **Media Resource Activity Configuration** form.
3. Specify the details in the value box for each of the parameters.
4. Click **Save/Save and close**.

Configuring Media Resource Activity Monitoring Settings

The Media Resource Activity Configuration page helps you to configure the media resource activity monitoring settings such as specifying threshold settings to generate incidents (if you launch this form from the details form of a media device), enabling monitoring for media resource activity, and enabling reporting for media resource activity.

To configure the monitoring of media resource activity:

1. Click  **New**. This opens the Media Resource Activity Configuration form.
2. On the Media Resource Activity Configuration form, under the Configurations for Media Device: *<Name of the cluster>* section, specify the following details in the value box for each of the following parameters:
 - **Measurement Type:** specify the type of resource activities to be configured from the drop-down list. The drop-down list displays the following resource activities:
 - Active Resources: The number of resources that are currently in use.
 - Unavailable Resources: 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: The number of resources that are available to be used. These resources are not in use at the current time.
- Total Resources: The total number of resources.
- **Enable Monitoring:** Select Enable Monitoring to configure the NNM iSPI for IP Telephony to start monitoring the media resource activity.
- **Enable Reporting:** Select Enable Reporting to configure the NNM iSPI for IP Telephony to start generating the reports of media resource activity monitoring.
- **Threshold Check:** Select this check box to specify the threshold settings that you want to configure for the media resource activity.

Note: You cannot configure thresholds for media devices if you launch Monitoring Configuration form for a cluster. You have to set thresholds for all media devices separately. Launch Monitoring Configuration form from the details form of each media device to set thresholds for the resources in that particular media device.

- **Threshold Severity:** Select one of the following options from the Severity drop-down list to configure the severity of the incident that must be generated during a threshold violation. Based on your selection, the NNM iSPI for IP Telephony generates the incident listed adjacent to the severity level below in parenthesis:
 - **Critical:** (*MonitoredAttributeThresholdBreachCritical*)
 - **Major:** (*MonitoredAttributeThresholdBreachMajor*)
 - **Minor:** (*MonitoredAttributeThresholdBreachMinor*)
 - **Warning:** (*MonitoredAttributeThresholdBreachWarning*)

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 listed

- **Lower Base:** Type the lower value for the media resource activity threshold.
- **% Lower Deviation:** Type the acceptable percentage of deviation from the lower base threshold value before generating an incident.
- **Abs Lower Deviation:** Type the acceptable absolute value of deviation from the lower base threshold value before generating the incident.
- **Lower Trigger Count:** Type the minimum threshold violation count. The NNM iSPI for IP Telephony generates the incident when the threshold violation occurs consecutively for the value specified in this box. Specifying the trigger count is mandatory for generating incidents.
- **Higher Base:** Type the higher value for the media resource activity threshold.
- **% Higher Deviation:** Type the acceptable percentage of deviation from the higher base

threshold value before generating an incident.

- **Abs Higher Deviation:** Type the acceptable absolute value of deviation from the higher base threshold value before generating the incident.
- **Higher Trigger Count:** Type the maximum threshold violation count. The NNM iSPI for IP Telephony generates the incident when the threshold violation occurs consecutively for the value specified in this box. Specifying the trigger count is mandatory for generating incidents.

3. Click **Save/Save and close**.

To delete a media resource activity monitoring configuration, see ["To delete a media resource activity monitoring configuration:"](#):

To modify a media resource activity monitoring configuration, see ["To modify a media resource activity monitoring configuration:"](#):

Configure Gateway Call Activity Monitoring

The NNM iSPI for IP Telephony allows you to monitor the active calls handled by the gateways in your network. You can monitor the call activity for the following types of gateway entities:

- H.323 gateway box
- MGCP gateway interfaces

You can specify the threshold deviation to be monitored for the active calls on the gateway or the gateway interface to generate incidents if thresholds are violated. You can also enable reporting based on the active calls handled by the gateway.


You must perform the following tasks to configure gateway call activity monitoring settings:

1. Configure gateway call activity monitoring settings as shown in the following section.
2. Configure gateway call activity configuration settings. See the [Configuring Gateway Call Activity Monitoring](#) section for more details.

To configure the gateway call activity monitoring for a cluster:

1. From the NNMi console, click the **Cisco IP Telephony** workspace on the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view
3. Select a cluster and click **Actions > IP Telephony > Monitoring Configuration** from the menu to launch the Monitoring Configuration for UCM cluster page for the UCM cluster.
4. Select **Gateway Call Activity** from the **Area of Monitoring** drop-down list. The right pane displays the resources configured for monitoring.
5. Select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The iSPI for IP Telephony uses this value to monitor the call activity periodically.
6. Select **Apply Configuration Setting to Other UCM Clusters** option if you want the call activity monitoring settings to be applied on other clusters.
7. Specify the common custom information configured for the other clusters in the box provided.

Note: You can alternatively launch the Monitoring Configuration for UCM Cluster page by right clicking a cluster from the UCM Clusters view and selecting **IP Telephony > Monitoring Configuration** from the menu.


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

The right pane on the Monitoring Configuration for UCM Cluster page displays the list of existing gateway call activity configuration settings under the Gateway Call Activity tab along with the attributes enabled for each activity configuration. A tick mark below the attribute indicates that the attribute is enabled for the gateway call activity configuration.


The iSPI for IP Telephony applies the call activity settings configured for a cluster to all the MGCP gateway interfaces and the H.323 gateway boxes in the cluster. The iSPI for IP Telephony allows you to configure active call monitoring for each gateway. If you specify the active call monitoring for the cluster after specifying the active call configuration settings for the gateway in the cluster, then the settings specified for the cluster overrides the settings specified for the individual gateways.

To configure the gateway call activity monitoring for a cluster:

1. From the NNMi console, click the **Cisco IP Telephony** workspace on the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view
3. Double-click a cluster and open the Cluster Details form.
4. Based on your requirement to monitor the active calls on an H.323 gateway box or an MGCP gateway interface, do one of the following to open the respective Voice Gateway form from the Cluster Details form:
 - a. Double click a gateway from the H.323 Gateways tab
 - b. Double click an MGCP interface from the MGCP/SCCP Gateways tab.
5. Click **Actions > IP Telephony > Monitoring Configuration** from the menu to launch the Monitoring Configuration for Cisco Voice Gateway page.
6. Follow steps 4 through 8 in the previous procedure to complete the configuration.


To add call activity configuration for a gateway, click  (New) from the right pane on the Monitoring Configuration for UCM Cluster page. See the [Configuring Gateway Call Activity Monitoring](#) section for more details.

To delete a gateway call activity monitoring configuration:

1. On the Monitoring Configuration for UCM Cluster form, select the check box of the gateway call activity monitoring configuration that you want to delete.
2. Click  Delete to delete the gateway call activity monitoring configuration.

Tip: You can delete all gateway call activity monitoring configurations by clicking **Delete All**. You can disable all gateway call activity monitoring configurations by clicking **Disable All**.


To modify a gateway call activity monitoring configuration:

1. On the Monitoring Configuration for UCM Cluster form, select the check box of the gateway call activity monitoring configuration that you want to modify.
2. Click  Edit. This opens the Gateway Call Activity form.
3. Specify the details in the value box for each of the parameters.
4. Click **Save/Save and close**.

Configuring Gateway Call Activity Monitoring Settings for a Cluster

The Monitoring Configuration for UCM Cluster page allows you to specify the configuration settings to monitor the active calls at the cluster level.

To configure the monitoring of gateway call activity:

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 **Actions > IP Telephony > Monitoring Configuration**. The Monitoring Configuration for UCM Cluster form opens.
3. Select **Gateway Call Activity** from the **Area of Monitoring** drop-down list.
4. Click **New** . This opens the Gateway Call Activity form.
5. On the gateway Call Activity form, specify the following details in the value box for each of the following parameters:
 - **Measurement Type**: select Gateway Active Calls from this drop-down list.
 - **Enable Monitoring**: select this option if you want to enable monitoring of active calls for the selected cluster.
 - **Enable Reporting**: select this option to enable reporting based on the active calls handled by the gateway on the cluster.
6. Click **Save**.

Note: At the cluster level, you can enable reporting and monitoring for the active calls handled by the gateway boxes or gateway interfaces in the cluster.


Configuring Gateway Call Activity Monitoring for a Gateway Interface

The Monitoring Configuration for Cisco Voice Gateway page allows you to specify the configuration settings to monitor the active calls on a gateway box or a gateway interface.

The monitoring of the count of active calls through a gateway enables you to configure thresholds for the active calls. The NNM iSPI for IP Telephony generates incidents when the thresholds are violated.

To configure the monitoring of gateway call activity:

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > UCM Clusters**. The UCM Clusters view opens in the right pane.
2. Select a cluster and double click the cluster to open the Cluster Details form for that cluster.

3. Double-click a cluster and open the Cluster Details form.
4. Based on your requirement to monitor the active calls on an H.323 gateway box or an MGCP gateway interface, do one of the following to open the respective Voice Gateway form:
 - a. Double click an MGCP interface from the **MGCP/SCCP Gateways** tab.
 - b. Double click a gateway from the **H.323 Gateways** tab
5. Click **Actions > IP Telephony > Monitoring Configuration** from the menu to launch the Monitoring Configuration for Cisco Voice Gateway page.
6. Click **New** . This opens the Gateway Call activity for Cluster page.
7. Specify the following details in the value box for each of the following parameters:
 - **Measurement Type**: select Gateway Active Calls from this drop-down list.
 - **Enable Monitoring**: select this option if you want to enable monitoring of active calls for the selected gateway interface.
 - **Enable Reporting**: select this option to enable reporting based on the active calls handled by the gateway interface.
8. Select **Generate Incident** if you want the iSPI for IP Telephony to generate an incident in the event of a threshold violation.
9. Select one of the following options from the **Threshold Severity** drop-down list to configure the severity of the incident that must be generated during a threshold violation. Based on your selection, the NNM iSPI for IP Telephony generates the incident listed adjacent to the severity level below in parenthesis:
 - **Critical**: (*MonitoredAttributeThresholdBreachCritical*)
 - **Major**: (*MonitoredAttributeThresholdBreachMajor*)
 - **Minor**: (*MonitoredAttributeThresholdBreachMinor*)
 - **Warning**: (*MonitoredAttributeThresholdBreachWarning*)

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 listed

10. Specify the following details in the value box for each of the following parameters:
 - **Lower Base**: Type the lower value for the media resource activity threshold.
 - **% Lower Deviation**: Type the acceptable percentage of deviation from the lower base threshold value before generating an incident.
 - **Abs Lower Deviation**: Type the acceptable absolute value of deviation from the lower base threshold value before generating the incident.
 - **Lower Trigger Count**: Type the minimum threshold violation count. The NNM iSPI for IP Telephony generates the incident when the threshold violation occurs consecutively for the value specified in this box. Specifying the trigger count is mandatory for generating incidents.
 - **Higher Base**: Type the higher value for the media resource activity threshold.

- **% Higher Deviation:** Type the acceptable percentage of deviation from the higher base threshold value before generating an incident.
- **Abs Higher Deviation:** Type the acceptable absolute value of deviation from the higher base threshold value before generating the incident.
- **Higher Trigger Count:** Type the maximum threshold violation count. The NNM iSPI for IP Telephony generates the incident when the threshold violation occurs consecutively for the value specified in this box. Specifying the trigger count is mandatory for generating incidents.

11. Click **Save/Save and close**.


Note: You can configure the active call monitoring at the gateway interface level only if you have configured active call monitoring at the cluster level.

Note: The **New *** option on the Gateway Call Activity form at the gateway interface level allows you to add any gateway interfaces that were added after you configured the active call configuration for the cluster.


Configure Monitoring of the Call Manager Administration Web Page Availability

The iSPI for IP Telephony allows you to monitor the availability of the administration web page for a call manager. You can configure the iSPI for IP Telephony to generate incidents based on the availability of the web page.


To configure the monitoring of the call manager administration web page state:

1. From the NNMi console, click the **Cisco IP Telephony** workspace on the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view.
3. Select a cluster and double click the cluster to open the cluster details form.
4. Select a UCM from the list of UCMs listed under the UCM tab and double click the UCM to open the UCM Details form.
5. Click **Actions > IP Telephony > Monitoring Configuration** from the menu to launch the Monitoring Configuration for UCM page for the UCM.
6. Select **Availability** from the Area of Monitoring drop-down list.
7. Select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The iSPI for IP Telephony uses this value to monitor the state of the administration web page for the call manager.
8. Click  (Save) to save the monitoring configuration.

The right pane on the Monitoring Configuration for UCM page displays the list of existing administration web page monitoring configuration settings under the **Availability** tab along with the attributes enabled for monitoring configuration. A tick mark below the attribute indicates that the attribute is enabled for the monitoring configuration.


To add administration web page state monitoring configuration settings, click  (New) from the right pane on the Monitoring Configuration for UCM page. See the [Configure Monitoring of Call Manager Administration Web Page state](#) section for more details.

To delete a monitoring configuration:

1. On the Monitoring Configuration for UCM form, select the check box of the monitoring configuration that you want to delete.
2. Click  Delete to delete the monitoring configuration.

Tip: You can delete all monitoring configuration settings by clicking **Delete All**. You can disable all monitoring configuration settings by clicking **Disable All**.


To modify a monitoring configuration:

1. On the Monitoring Configuration for UCM form, select the check box of the monitoring configuration that you want to modify.
2. Click  Edit. This opens the **Availability for Cisco Call Manager** form.
3. Specify the details in the value box for each of the parameters.
4. Click **Save/Save and close**.


Configure Monitoring of Call Manager Administration Web Page State Settings

The Availability for Cisco Call Manager page helps you to configure the monitoring of the availability of the administration web page for the selected call manager.


To configure the administration web page availability for a call manager:

1. Click  (New) from the right pane on the Monitoring Configuration for UCM page. This opens the Availability for Cisco Call Manager page.
2. Select **CCM Admin Web Page** from the Measurement Type drop-down list.
3. Select **Enable Monitoring** to configure the iSPI for IP Telephony to start monitoring the availability of the administration web page for the call manager.
4. Select **Generate Incident** to specify that an incident must be generated if there is a change in the threshold state configured for the administration web page .
5. Select one of the following options from the **Threshold Severity** drop-down list to configure the severity of the incident that must be generated during a threshold violation. Based on your selection, the iSPI for IP Telephony generates the incident listed adjacent to the severity level below in parenthesis:
 - **Critical:** (*MonitoredAttributeThresholdBreachCritical*)
 - **Major:** (*MonitoredAttributeThresholdBreachMajor*)
 - **Minor:** (*MonitoredAttributeThresholdBreachMinor*)
 - **Warning:** (*MonitoredAttributeThresholdBreachWarning*)

Note: The iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents listed.

6. Select one of the following options from the **Threshold State** drop-down list:
 - **Available**: specifies that the administration web page for the call manager is available.
 - **Not Available**: specifies that the administration web page for the call manager is not available.
7. Click  (Save) to save the configuration settings.

For example, if you want the iSPI for IP Telephony to generate the *MonitoredAttributeThresholdBreachCritical* incident when the administration web page for the call manager is not available, select the following options after performing step 1 through step 4 from the procedure listed:

1. Select **Critical** from the **Threshold Severity** drop-down list.
2. Select **Not Available** from the **Threshold State** drop-down list.
3. Click  (Save) to save the configuration settings.

Monitor the Health of Cisco Unified Communications Managers

The NNM iSPI for IP Telephony enables you to monitor the following parameters of Cisco Unified Communications Manager that indicate the health of the system:

Cisco Unified Call Manager System Health Monitoring Parameters

System Health Parameter	Description
Active partition used	Total space in use by the active partition
Common partition used	Total space in use by the common partition
CPU time	CPU utilization of the Cisco Unified Communications Manager
Memory used	Memory utilization of the Cisco Unified Communications Manager
Process: ccm - CPU time	CPU utilization of the ccm process
Process: ccm - memory used	Memory utilization of the ccm process
Swap partition used	Total space in use by the swap partition
Swap space used	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	Time elapsed since the last reboot.
Total processes	Total number of processes on the Cisco Unified Communications Manager

System Health Parameter	Description
Total threads	Total number of threads on the Cisco Unified Communications Manager
VM used	Total virtual memory in use

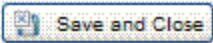
You must perform the following tasks to be able to monitor this:

1. ["Enable Monitoring" \(on page 123\)](#)
2. ["Select System Health Parameters for Monitoring" \(on page 123\)](#)

Enable Monitoring

The Monitoring Configuration feature enables you to configure monitoring of system health parameters of Cisco Unified Communications Managers.

To enable monitoring of system health parameters:

1. Log on to the NNMi console as an administrator.
2. Navigate to the Monitoring Configuration for the UCM form.
 - a. From the NNMi workspace, click **Cisco IP Telephony > UCM Clusters**.
 - b. In the UCM Clusters inventory, double-click a Cisco Unified Communications Manager cluster of your choice.
 - c. In the UCM Cluster Details form, double-click a Cisco Unified Communications Manager of your choice. The Cisco Call Controller Details form opens.
 - d. In the Cisco Call Controller Details form, click **Actions > IP Telephony > Monitoring Configuration**. The Monitoring Configuration for UCM form opens.
3. In the left pane, select **System Health** in the Area of Monitoring box.
4. Specify a value in the Collection Interval box. To gather system health details, the NNM iSPI for IP Telephony polls the selected Cisco Unified Communications Manager at the interval you specify here.
5. The NNM iSPI for IP Telephony does not support exporting of Cisco Unified Communications Manager system health data to the CSV format. Leave the CSV export interval box blank.
6. Click  **Save and Close**.


Now you must select system health parameters that you want to monitor. Use the [Add System Health](#) form to select system health parameters of your choice.

Select System Health Parameters for Monitoring

The Add System Health form enables you to select system health parameters for monitoring. This form provides you with a list of system health parameters of Cisco Unified Communications Manager to choose from. You can use the following mechanisms of monitoring:

- Reporting (for viewing reports using the NPS)
- Generating incidents (for viewing incidents in the incident browser)

To select system health parameters for monitoring:

1. Log on to the NNMi console as an administrator.
2. Navigate to the Monitoring Configuration for UCM form.
 - a. From the NNMi workspace, click **Cisco IP Telephony > UCM Clusters**.
 - b. In the UCM Clusters form, double-click a Cisco Unified Communications Manager cluster of your choice.
 - c. In the UCM Cluster Details form, select a Cisco Unified Communications Manager of your choice, and then click **Actions > IP Telephony > Monitoring Configuration**. The Monitoring Configuration for UCM form opens.
3. Go to the System Health tab.
4. In the right pane, click  **New**. The Add System Health form opens.
5. In the Add System Health form, select a system health parameter in the Measurement Type list (see [Monitor the Health of Cisco Unified Communications Managers](#) for a complete list of system health parameters).

If you select system reboot:

- a. Select the Enable Monitoring check box.
- b. Select the Enable Reporting check box if you use the NNM iSPI Performance for Metrics.
- c. Select the Generate Incidents check box if you want to generate incidents for threshold violation (that is, when the Cisco Unified Communications Manager is restarted).
- d. Select the severity of the threshold.

If you select system uptime, select the Enable Monitoring check box. The NNM iSPI for IP Telephony indicates the availability status and availability history of the system in the analysis pane if you select this check box.

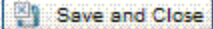
If you select a parameter other than system reboot or system uptime:

- a. Select the Enable Monitoring check box.
- b. Select the Enable Monitoring check box.
- c. Select the Enable Reporting check box if you use the NNM iSPI Performance for Metrics.

Note: Exporting of the system health data to CSV files is not supported.



- d. Select the Generate Incidents check box if you want to generate incidents for threshold violation.
- e. Specify the following details for configuring a threshold range for incident generation:

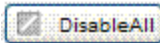
Threshold Element	Description
Threshold Severity	Specifies the severity of the incident
Lower Base	Specifies the lower limit of the threshold range
% Lower Deviation	Specifies the acceptable percentage of deviation from the lower base threshold value before generating an incident
Abs Lower Deviation	Specifies the acceptable absolute value of deviation for the lower base threshold value before generating the incident
Lower Trigger Count	The number of consecutive times the returned value must fall below the specified Lower Base to trigger an incident.
Higher Base	Specifies the upper limit of the threshold range
% Higher Deviation	Specifies the acceptable percentage of deviation from the higher base threshold value before generating an incident
Abs Higher Deviation	Specifies the acceptable absolute value of deviation for the higher base threshold value before generating the incident
Higher Trigger Count	The number of consecutive times the returned value must exceed the specified Higher Base to trigger an incident.

6. Click  **Save and Close**. A new element appears in the right pane in the System Health tab of the Monitoring Configuration for UCM form.
7. Perform this procedure for every system health parameter you want to monitor.

You can update an existing configuration with the same form (Add System Health).

To delete a system health parameter:

Select the parameter in the System Health tab, and then click  **Delete**. To delete all the parameters, click  **Delete All**.

You can also disable monitoring of all configured parameters by clicking  **Disable All**.

Configure Monitoring of Availability of Services on the UCM

The iSPI for IP Telephony allows you to monitor the state of the services on a UCM. You can configure the iSPI for IP Telephony to generate incidents based on the state of the services. You can configure the iSPI for IP Telephony to generate incidents if the state of the service changes from *Started* to *Stopped*, *Activated* to *Deactivated* or in the reverse scenarios.

Note: The iSPI for IP telephony allows you to monitor the availability of the services currently on the discovered UCM.


You must perform the following tasks to configure service availability monitoring:

1. Configure SSH credentials for all the Cisco Unified Communication Managers in the cluster that you want to monitor. See the section "[Configuring Data Access for Cisco](#)" (on page 245) for more details.
2. Configure monitoring of the availability of services as shown in the following section.
3. Configure service availability configuration settings. See [Settings for Availability of Services on the UCM](#) for more details.


To configure the monitoring of the availability of the services:

1. From the NNMI console, click the **Cisco IP Telephony** workspace on the left pane.
2. Click **UCM Clusters** from the list of options listed. This displays the UCM Clusters view
3. Select a cluster and double click the cluster to open the cluster details form.
4. Select a UCM from the list of UCMs listed under the UCM tab and double click the UCM to open the UCM Details form.
5. Click **Actions > IP Telephony > Monitoring Configuration** from the menu to launch the Monitoring Configuration for UCM page for the UCM.
6. Select **Services** from the Area of Monitoring drop-down list.


Note: You can alternatively click the **Services** tab on the right pane.

7. Select minutes (**mins**) or hours (**hrs**) from the **Collection Interval** drop-down list and specify the value in the respective box. The iSPI for IP Telephony uses this value to monitor the availability of the service on the call manager.
8. Click  (Save) to save the monitoring configuration.

The right pane on the Monitoring Configuration for UCM page displays the list of existing service availability configuration settings under the **Availability** tab along with the attributes enabled for monitoring configuration. A tick mark below the attribute indicates that the attribute is enabled for the monitoring configuration.


To add service availability monitoring configuration settings, click  (New) from the right pane on the Monitoring Configuration for UCM page. See the [Settings for Availability of Services on the UCM](#) section for more details.

To delete a monitoring configuration:

1. On the Monitoring Configuration for UCM form, select the check box of the monitoring configuration that you want to delete.
2. Click  Delete to delete the monitoring configuration.

Tip: You can delete all monitoring configuration settings by clicking **Delete All**. You can disable all monitoring configuration settings by clicking **Disable All**.


To modify a monitoring configuration:

1. On the Monitoring Configuration for UCM form, select the check box of the monitoring configuration that you want to modify.
2. Click  Edit. This opens the **UCOS Service Availability Configuration for Call Manager** form.
3. Specify the details in the value box for each of the parameters.
4. Click **Save/Save and close**.

Settings for Availability of Services on the UCM

The UCOS Service Availability Configuration for call manager form helps you to configure the service availability monitoring 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.

Note: You must configure the NNM iSPI for IP Telephony to access data from the Cisco Unified Communications Managers by using SSH. See ["Access the Cisco Unified Communications Manager with SSH" \(on page 254\)](#) for more information about configuring the NNM iSPI for IP Telephony to use SSH.

1. Click  (New) from the right pane on the Monitoring Configuration for UCM Cluster page. This opens the UCOS Service Availability Configuration for call manager form.
2. Select the service to be monitored from the **Measurement Type** drop-down list. You can select multiple services from the drop-down list by pressing the Control (Ctrl) key. Alternatively, you can click **All** to select all the listed services on the UCM.
3. Select **Enable Monitoring** to configure the iSPI for IP Telephony to start monitoring the selected service.
4. Select **Enable Reporting** to configure the iSPI for IP Telephony to start reporting based on the selected service.
5. Select **Generate Incident** to generate the incident in the event of a state change for the service being monitored.
6. Select one of the options from the **State** drop-down list:
 - Started
 - Stopped
 - Activated
 - Deactivated
7. Select one of the following options from the **Threshold Severity** drop-down list to configure the severity of the incident that must be generated during a service state change. Based on your selection, the iSPI for IP Telephony generates the incident listed adjacent to the severity level below in parenthesis:
 - **Critical:** (*MonitoredAttributeThresholdBreachCritical*)
 - **Major:** (*MonitoredAttributeThresholdBreachMajor*)

- **Minor:** (*MonitoredAttributeThresholdBreachMinor*)
- **Warning:** (*MonitoredAttributeThresholdBreachWarning*)

Note: The iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachClear* incident after you resolve the cause for the generation of any of the four incidents listed.

8. Click **Save**.

For example, consider that you have configured the following service availability settings to monitor a service on the UCM:

1. Select the **Enable Monitoring** option
2. Select the **Generate Incident** option
3. Select **Stopped** from the **State** drop-down list
4. Select **Critical** from the **Threshold Severity** drop-down list.
5. Click **Save**.

In this scenario, the iSPI for IP Telephony generates the *MonitoredAttributeThresholdBreachCritical* when the monitored service changes its state to *Stopped*.

Guidelines

- You must always configure the monitoring of measurement attributes for the Cisco Unified Communications Manager cluster first, and then for the underlying Cisco Unified Communications Managers and components.
- To enable monitoring and reporting of a specific attribute for a Cisco Unified Communications Manager, you must make sure that the monitoring and reporting of the same attribute are configured for the hosting cluster as well.
- Deleting a measurement attribute for a Cisco Unified Communications Manager cluster results in automatic deletion of the same attribute for underlying Cisco Unified Communications Managers.
- Threshold settings of an attribute on a Cisco Unified Communications Manager cluster can be different from the threshold settings of the same attribute on an underlying Cisco Unified Communications Manager.
- On a newly discovered Cisco Unified Communications Manager, UCM Subscriber Group, or device pool, enabling the monitoring of a measurement attribute does not take effect unless the hosting Cisco Unified Communications Manager cluster is configured to monitor the same measurement attribute.

ClarusIPC Integration—Test Plans and Test Result Reports

The integration of 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 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 for Cisco" \(on page 245\)](#) section before viewing this report.
- You must configure Cisco CDR access configuration as specified in the ["Configuring Data Access for Cisco" \(on page 245\)](#) section before viewing this report.
- You must enable CDR-based reporting as specified in the ["Configure Cisco IP Telephony CDR-based Reporting" \(on page 287\)](#) 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: It is recommended to provide a gap of a day or more between the start date and the end date to generate reports. By default, the iSPI for IP Telephony generates the report for the past one week.

- **Direction:** Select one of the following options to specify the type of 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.
 - **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: You can click the **GOS Reference Chart** to see a chart that lists the number of channels

and the recommended GoS score for those 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" \(on page 129\)](#)

- You must configure Cisco AXL Data access configuration as specified in the ["Configuring Data Access for Cisco" \(on page 245\)](#) section before viewing this report.
- You must configure Cisco CDR access configuration as specified in the ["Configuring Data Access for Cisco" \(on page 245\)](#) section before viewing this report.
- You must enable CDR-based reporting as specified in the ["Configure Cisco IP Telephony CDR-based Reporting" \(on page 287\)](#) 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: It is recommended to provide a gap of a day or more between the start date and the end date to generate reports. By default, the iSPI for IP Telephony generates the report for the past one week.

- **Direction:** Select one of the following options to specify the type of 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.
- **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: You can click the **GOS Reference Chart** to see a chart that lists the number of channels and the recommended GoS score for those number of channels.

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	<p>The status of the Nortel Call Server. Possible values are:</p> <ul style="list-style-type: none"> • No Status • Normal • Disabled • Warning • Minor • Major • Critical • Unknown
Name	The system name of the Nortel Call Server.


Attribute	Description
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	<p>The management server for the call server. This attribute displays one of the following values:</p> <ul style="list-style-type: none"> • 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:

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.

Attribute	Description
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: <ul style="list-style-type: none"> • 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:


Attribute	Description
	<ul style="list-style-type: none">• 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:

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.

Attribute	Description
Description	A short description of the server.
Model	Model of the Nortel Signaling Server.
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: <ul style="list-style-type: none">• 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:

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.

Attribute	Description
Intervalln	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.
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.

Attribute	Description
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

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

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:

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.
IP Address	The IP address of the phone.
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.


Attribute	Description
Description	A description of the media gateway device.
Management Server	<p>The management server for the media gateway device. This attribute displays one of the following values:</p> <ul style="list-style-type: none"> • 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.

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: <ul style="list-style-type: none">• Active—indicates the call controller is in the active state.

Attribute	Description
	<ul style="list-style-type: none"> Standby—indicates that the call controller is in the standby state. Unknown—indicates that the status of the call controller is currently unknown.
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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.

Attribute	Description
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: <ul style="list-style-type: none"> Managed: indicates that the node is managed by the iSPI for IP Telephony. Out of Service: indicates that the node is currently out of service and not managed by the iSPI for IP Telephony. Unmanaged: indicates that the node is currently not managed by the 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.
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.

Attribute	Description
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.
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.

Attribute	Description
RSVP Profile	Lists the RSVP profile. The profile can be one of the following: <ul style="list-style-type: none">• 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.
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.

Metric	Description
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 iSPI for IP Telephony compares the metric with the specified value. If the value exceeds the specified threshold value, the 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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.
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 hostname for the route pattern.
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.
Management Mode	Displays the management state of the route pattern. The status can be one of the following strings: <ul style="list-style-type: none">• Managed: indicates that the route pattern is managed by the iSPI for IP Telephony.• Out of Service: indicates that the route pattern is currently out of service and not managed by the iSPI for IP Telephony.• Unmanaged: indicates that the route pattern is currently not managed by the 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.
Calls Offered	The total number of calls offered to the route pattern.
Calls Carried	The total number of seizures (resources in the trunk groups used) by calls for all the trunk groups in the route pattern.

Attribute	Description
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 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.
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	You can specify the queue overflow threshold in the box provided. You must click the Save and Close button on the menu bar to apply the threshold value.


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

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 hostname of the trunk group.
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.
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  (Save) 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 number of times a trunk was seized in the group.

Attribute	Description
Incoming Seize	The total number of incoming seizures on the trunk group.
Group Overflow	The total number of calls to a trunk group that were not placed in a queue or carried.
Queue Size	The number of slots assigned to the trunk group queue.
Queue Overflow	The total number of calls that were not queued as the queue was full.
Queue Abandoned	The total number of calls that were removed from the queue.
Out of Service	The total number of trunks in the trunk group that are out of service due to maintenance.
%ATB	The percentage of time when all the trunks in the group were busy.
%Out Block	The percentage of calls that were offered to the trunk group, but was not carried on the trunk group.


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

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 hostname 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.

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.

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.

Attribute	Description
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.
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 iSPI for IP Telephony compares the metric with the specified value. If the value exceeds the specified threshold value, the iSPI for IP Telephony generates an incident on the Incidents tab page of the Avaya Call Controller form.


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.
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:

Attribute	Description
	<ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Managed: indicates that the IPSI is managed by the iSPI for IP Telephony.• Out of Service: indicates that the IPSI is currently out of service and not managed by the iSPI for IP Telephony.• Unmanaged: indicates that the IPSI is currently not managed by the 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: <ul style="list-style-type: none">• Managed: indicates that the CLAN is managed by the iSPI for IP Telephony.• Out of Service: indicates that the CLAN is currently out of service and not managed by the iSPI for IP Telephony.• Unmanaged: indicates that the CLAN is currently not managed by the 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.
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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• Managed: indicates that the media processor is managed by the iSPI for IP Telephony.• Out of Service: indicates that the media processor is currently out of service and not managed by the iSPI for IP Telephony.• Unmanaged: indicates that the media processor is currently not managed by the 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.
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.

General Attribute	Description
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: <ul style="list-style-type: none"> • 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 iSPI for IP Telephony compares the metric with the specified value. If the value exceeds the specified threshold value, the 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:

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 with its current controller. Possible values are: <ul style="list-style-type: none">RegisteredUnregistered
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.

Attribute	Description
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	<p>The management server for the IP phone. This attribute displays one of the following values:</p> <ul style="list-style-type: none">• 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 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 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:

1. **Right-click the Registration State, Extension Number, IP Address, Tenant, Controller , or Management Server** attribute of one of the IP phones listed in the Avaya 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 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**.

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: <ul style="list-style-type: none">• Managed: indicates that the IP Phone is managed by the iSPI for IP Telephony.• Out of Service: indicates that the IP Phone is currently out of service and not managed by the iSPI for IP Telephony.• Unmanaged: indicates that the IP Phone is currently not managed by the iSPI for IP Telephony.
Registration State	The registration state of the IP phone.
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.

Attribute	Description
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:


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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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:

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.
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: <ul style="list-style-type: none">• Managed: indicates that the media gateway is managed by the iSPI for IP Telephony.• Out of Service: indicates that the media gateway is currently out of service and not managed by the iSPI for IP Telephony.• Unmanaged: indicates that the media gateway is currently not managed by the 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.

Attribute	Description
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.
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:

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: <ul style="list-style-type: none">• Managed: indicates that the media module is managed by the iSPI for IP Telephony.• Out of Service: indicates that the media module is currently out of service and not managed by the iSPI for IP Telephony.• Unmanaged: indicates that the media module is currently not managed by the 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.

Attribute	Description
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.
Management Mode	Displays the management state of the VOIP engine. The status can be one of the following strings: <ul style="list-style-type: none">• Managed: indicates that the VOIP engine is managed by the iSPI for IP Telephony.• Out of Service: indicates that the VOIP engine is currently out of service and not managed by the iSPI for IP Telephony.• Unmanaged: indicates that the VOIP engine is currently not managed by the 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.

Attribute	Description
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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">Managed: indicates that the DSP core is managed by the iSPI for IP Telephony.Out of Service: indicates that the DSP core is currently out of service and not managed by the iSPI for IP Telephony.Unmanaged: indicates that the DSP core is currently not managed by the iSPI for IP Telephony.
VOIP Engine IP Address	The IP address of the VOIP engine associated with the DSP core.
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.

Incidents Collected from the ClarusIPC Environment

If you integrate the ClarusIPC deployment with the 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

Incident	Message	Severity	Description
			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.
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 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.

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).
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;	Critical	This incident indicates that the Unified

Cisco IP Telephony Incident	Message	Severity	Description
	Subscriber Group (CUCM Priority): \$cmGrpAndPriority.		Communications Operating System (UCOS) CallManager service is down.
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.
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

Cisco IP Telephony Incident	Message	Severity	Description
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.
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.
CallTerminationReason	Termination reason is "\$terminationReason" for	Warning	This incident is generated when the

Cisco IP Telephony Incident	Message	Severity	Description
	call from \$callingPartyNumber to \$finalCalledPartyNumber in Cluster \$clusterId from device "\$origEndpointName" to device "\$destEndpointName".		user-specified call termination cause code to be monitored, matches with a call termination cause code.
MonitoredAttributeThresholdBreachCritical	\$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.
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.

Nortel IP Telephony Incidents Generated by the NNM iSPI for IP Telephony

Nortel IP Telephony Incident	Message	Severity	Description
callsMadeInViolation	The Intra QOS Zone	Critical	The Intra QOS Zone

Nortel IP Telephony Incident	Message	Severity	Description
	callsMadeIn parameter has violated set threshold value.		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 peakOut parameter has violated set threshold value.	Critical	The Inter QOS Zone peakOut 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.
avgOutViolated	The Inter QOS Zone avgOut parameter has violated set threshold value.	Critical	The Inter QOS Zone avgOut parameter has violated set threshold value.

Nortel IP Telephony Incident	Message	Severity	Description
	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.
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	Critical	The Intra QOS Zone unacpJitterIn parameter has violated set threshold value.

Nortel IP Telephony Incident	Message	Severity	Description
	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.
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.

Nortel IP Telephony Incident	Message	Severity	Description
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.
NortelISetStatusUnregistered	Nortel IP Phone Unregistered. Extension: \$extension. Signaling Server: \$sslIpAddress. 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	Critical	This trap is used to provide a real time indication of a critical alarm condition. The

Nortel IP Telephony Incident	Message	Severity	Description
	\$7. Alarm Type \$8. Probable Cause \$9. Alarm Data \$10.		variables listed in VARIABLES clause are defined in the <code>mgmt-info</code> 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 <code>mgmt-info</code> group and are present in all information alarms.
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 <code>mgmt-info</code> 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 <code>mgmt-info</code> 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 <code>mgmt-info</code> 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 <code>mgmt-info</code> group and are present in all information alarms.

Avaya IP Telephony Incidents Generated by the NNM iSPI for IP Telephony

Avaya IP Telephony Incident	Message	Severity	Description
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 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
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

Avaya IP Telephony Incident	Message	Severity	Description
			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
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	Warning	This incident is generated when the Intercom Intra PN Peg Parameter in the Avaya Port Network, has breached the

Avaya IP Telephony Incident	Message	Severity	Description
	measurement hour \$loadintMeasHour.		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
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

Avaya IP Telephony Incident	Message	Severity	Description
			Connection
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
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:	Warning	This incident is generated when

Avaya IP Telephony Incident	Message	Severity	Description
	\$cmIpAddress, Port Network: \$pnNumber Outgoing Trunk Load metric Incoming Use = \$loadoutOutIncomingUse for measurement hour \$loadoutMeasHour.		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
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

Avaya IP Telephony Incident	Message	Severity	Description
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
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 Incident	Message	Severity	Description
AvayaSuServerStatusActive	Survivable Service Active: Avaya Survivable 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
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	Warning	This incident is generated when the Tandem Trunk

Avaya IP Telephony Incident	Message	Severity	Description
	Network: \$pnNumber Tandem Trunk Load metric Intra PN Peg = \$loadtanTanIntraPNPeg for measurement hour \$loadtanMeasHour.		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
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

Avaya IP Telephony Incident	Message	Severity	Description
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.
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

Avaya IP Telephony Incident	Message	Severity	Description
avayaIPServerInterfaceUnknown	IPSI Service is in Unknown state: IPSI \$psiIP in Avaya Primary CM \$cmIpAddress Port network \$pnNumber.	Warning	The Avaya IP Server Interface (IPSI) Service State is in the Unknown state
avayaIPServerInterfaceOUT	Out of Service:IPSI \$psiIP 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
ProcTotalAttemptedCallsViolate	Threshold Breached: Avaya CM Server \$ipAddress Total Call Attempts Occupancy = \$currentValue for	Warning	Processor Total Call Attempts Occupancy has breached the threshold specified

Avaya IP Telephony Incident	Message	Severity	Description
	measurement hour \$procMeasHour.		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.
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	Warning	The Processor Outgoing Attempts Occupancy has

Avaya IP Telephony Incident	Message	Severity	Description
	Attempts Occupancy = \$currentValue for measurement hour \$procMeasHour.		breached the threshold specified by you on the Avaya Communication Manager.
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.
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	Warning	This incident is generated when the Avaya IP

Avaya IP Telephony Incident	Message	Severity	Description
	Network Region \$number CODEC/DSP resources metric Usage = \$ipdspUsage for measurement hour: \$dspMeasHour.		Media Processor DSP Resource Usage parameter has breached the threshold value you specified for an IP Network Region.
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.
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.

Avaya IP Telephony Incident	Message	Severity	Description
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.
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.
IPNetworkRegionG711OutViolate	Threshold Breached:Avaya Primary CM \$cmIpAddress Network Region \$number CODEC/DSP resources metric G711 Out Of Region Allocations = \$codecG711OutRegion	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource G711 Out Region Allocations parameter has

Avaya IP Telephony Incident	Message	Severity	Description
	for measurement hour: \$codecMeashour.		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.
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
IPNetworkRegionDSPInViolate	Threshold Breached:Avaya Primary CM \$cmIpAddress	Warning	This incident is generated when

Avaya IP Telephony Incident	Message	Severity	Description
	Network Region \$number CODEC/DSP resources metric InRegion Allocations = \$dspInRegion for measurement hour: \$dspMeasHour.		the Avaya IP Media Processor DSP Resource In Region Allocations parameter has breached the threshold value you specified for an IP Network Region

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	<ul style="list-style-type: none">• Control LAN Circuit Pack• Control LAN Ethernet• Control LAN Packet/Port
IP media processor	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 , Avaya IP phones. The report displays the jitter for the calls between the two selected phones.

To launch the graph to view the jitter:

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**. The line graph opens in a new window.

The **File > Export to CSV** option is not supported for this graph.

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 line graph for the selected Avaya phones.

Viewing the Graphs for Average Packet Loss

With the 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.

To launch the graph to view the jitter:

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 Avg Packet Loss**. The line graph opens in a new window.

The **File > Export to CSV** option is not supported for this graph.

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 line graph for the selected Avaya phones.

Viewing the Graph for the Average MOS

With the 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.

To launch the graph to view the jitter:

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 Avg MOS**. The line graph opens in a new window.

The **File > Export to CSV** option is not supported for this graph.

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 line graph for the selected Avaya phones.

Viewing the Graphs for Latency

With the 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.

To launch the graph to view the jitter:

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 Latency**. The line graph opens in a new window.

The **File > Export to CSV** option is not supported for this graph.

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 line graph for the selected Avaya phones.

Launch a Voice Path

With the iSPI for IP Telephony, you can launch the voice path between two Cisco or Avaya IP phones. 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:

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 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). 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:

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 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:

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 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 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:

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 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:

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.

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 iSPI for IP Telephony monitoring tasks
- QOS and MOS monitoring threshold configuration
- Reporting configuration
- Data access configuration
- Regional Manager configuration.

It is recommended to configure the settings listed above before you seed any IP Telephony nodes in NNMi and start to monitor these nodes using the iSPI for IP Telephony. You can however use the configuration forms to configure the settings or modify the existing settings even after seeding the IP Telephony nodes or when the iSPI for IP Telephony is operational.

To launch the IP Telephony Configuration forms:

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.

As an administrator you can also 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:

- [Monitoring Configuration](#)
- [Manage Discovery and Monitoring](#)
- [Delete IP Telephony Devices](#)
- [Enable Log File Tracing](#)
- [Integrate the iSPI Telephony with Clarus IPC](#)

Specify the Range of Extensions for Cisco, Avaya, and Nortel Phones to be Excluded from Monitoring

You can specify the range of extensions for phones to be excluded from being monitored for both Avaya and Cisco. You can also specify the range of Nortel extensions to be excluded from discovery and monitoring. After you specify the range of extensions for Avaya and Cisco, the 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. For Nortel IP phones specified in the exclusion list, the iSPI for IP Telephony does not monitor these phones and stops discovering these phones in the subsequent discovery cycles.

To specify the range of extensions for Cisco phones to be excluded:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration**. The NNM iSPI for IP Telephony Configuration form opens.
2. Click **IP Phone Exclusion Configuration**. The NNM iSPI for IP Telephony Phone Exclusion Configuration form opens.
3. Click the **Cisco** tab.
4. In the **Tenant** drop-down list, select the name of the tenant that contains the list of IP phones that you want to exclude.
5. In the **Cluster ID** box, type the ID of the cluster that contains the list of IP phones that you want to exclude.
6. In the **Filter** section, specify the extension range to be excluded. See the section "[To specifying the Range of Phones to be excluded:](#)" (on page 245) for more information about specifying extension ranges to be excluded.
7. 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 delete a range of Cisco extensions specified to be excluded:

1. Go to the NNM iSPI for IP Telephony Phone Exclusion Configuration form as specified in the previous section.
2. Click the **Cisco** tab.
3. From the **Current Configuration** section, select the configuration.
4. Click **Delete**.

To modify a range of Cisco extensions specified to be excluded:

1. Go to the NNM iSPI for IP Telephony Phone Exclusion Configuration form as specified in the previous section.
2. Click the **Cisco** tab.
3. From the **Current Configuration** section, select the configuration.
4. Click **Modify**.
5. In the **Filter** section, specify the extension range to be excluded. See the section "[To specifying the Range of Phones to be excluded:](#)" (on page 245) for more information about specifying extension ranges to be excluded.

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.

6. Click **Add/Modify**.

To specify the range of extensions for Avaya phones to be excluded:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration**. The NNM iSPI for IP Telephony Configuration form opens.
2. Click **IP Phone Exclusion Configuration**. The NNM iSPI for IP Telephony Phone Exclusion Configuration form opens.
3. Click the **Avaya** tab.
4. In the **CM IP Address** section, specify 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.

5. In the **Filter** section, specify the extension range to be excluded in the **Value** box. See the section "[To specifying the Range of Phones to be excluded:](#)" (on page 245) for more information about specifying extension ranges to be excluded.
6. Click **Add/Modify**.

The **Current Configurations** section lists the configured communication managers for which you want to exclude the list of phones.

To delete a range of Avaya extensions specified to be excluded:

1. Go to the NNM iSPI for IP Telephony Phone Exclusion Configuration form as specified in the previous section.
2. Click the **Avaya** tab.
3. From the **Current Configuration** section, select the **CM IP Address** that you configured.
4. Click **Delete**.

To modify a range of Avaya extensions specified to be excluded:

1. Go to the NNM iSPI for IP Telephony Phone Exclusion Configuration form as specified in the previous section.
2. Click the **Avaya** tab.
3. From the **Current Configuration** section, select the **CM IP Address** that you configured.
4. Click **Modify**.
5. In the **CM IP Address** section, specify the IP address of the communication manager for which you want to specify the list of phones to be excluded.
6. In the **Filter** section, specify the extension range to be excluded in the **Value** box. See the section ["To specifying the Range of Phones to be excluded:" \(on page 245\)](#) for more information about specifying extension ranges to be excluded.
7. Click **Add/Modify**.

To specify the range of extensions for Nortel phones to be excluded:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration**. The NNM iSPI for IP Telephony Configuration form opens.
2. Click **IP Phone Exclusion Configuration**. The NNM iSPI for IP Telephony Phone Exclusion Configuration form opens.
3. Click the **Nortel** tab.
4. In the **CS IP Address** section, specify the IP address of the Call Server for which you want to specify the list of phones to be excluded.
5. In the **Filter** section, specify the extension range to be excluded in the **Value** box. See the section ["To specifying the Range of Phones to be excluded:" \(on page 245\)](#) for more information about specifying extension ranges to be excluded from discovery and monitoring.
6. Click **Add/Modify**.

The **Current Configurations** section lists the configured call servers for which you want to exclude the list of phones to be monitored and discovered

To delete a range of Nortel extensions specified to be excluded from discovery and monitoring:

1. Go to the NNM iSPI for IP Telephony Phone Exclusion Configuration form.
2. Click the **Nortel** tab.
3. From the **Current Configuration** section, select the **CS IP Address** that you configured.
4. Click **Delete**.

To modify a range of Nortel extensions specified to be excluded:

1. Go to the NNM iSPI for IP Telephony Phone Exclusion Configuration form as specified in the previous section.
2. Click the **Nortel** tab.
3. From the **Current Configuration** section, select the **CS IP Address** that you configured.
4. Click **Modify**.

5. In the **CS IP Address** section, specify the IP address of the Call Server for which you want to specify the list of phones to be excluded.
6. In the **Filter** section, specify the extension range to be excluded in the **Value** box. See the section "[To specifying the Range of Phones to be excluded:](#)" (on page 245) for more information about specifying extension ranges to be excluded from discovery and monitoring.
7. Click **Add/Modify**.

To specifying the Range of Phones to be excluded:

You can specify the range of phones to be excluded as follows:

- Using 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 **Value** box.
- Using the wildcard character asterisk (*) 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 **Value** box.
- Using the wildcard character question mark (?) 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 **Value** box.

Note: You can type multiple exclusion conditions in the **Value** box for a specific cluster. You must use commas (,) to separate multiple exclusion conditions.

Configuring Data Access

You can use the NNM iSPI for IP Telephony Data Access Configuration form to configure the NNM iSPI for IP Telephony to access various categories of management data from the Cisco, Avaya, and Nortel IP Telephony servers in your deployment environment.

To access the Data Access Configuration form:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Data Access Configuration**. This opens the NNM iSPI for IP Telephony Data Access Configuration form.

Click the following links to know more about configuring data access for IP Telephony devices:

[Configuring Data Access for Cisco](#)

[Configuring Data Access for Avaya](#)

[Configuring Data Access for Nortel](#)

Configuring Data Access for Cisco

You can use the Data Access Configuration form to configure the 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 this form to add a configuration for a cluster, modify the configuration for an existing cluster, or delete an existing configuration for a cluster.

Configure the NNM iSPI for IP Telephony to Access the AXL Data

Configure AXL access if you want comprehensive CDR reporting (including details on how Cisco Unified Communications Managers are associated with cluster IPs). You may receive incomplete CDR reports if you do not configure AXL access.

To discover and monitor SRST nodes and device pools, you must configure the AXL access for the Cisco Unified Communications Manager publisher server of the cluster to which the SRST nodes and device pools are registered.

If you configure the AXL credentials of the publisher CUCM, the NNM iSPI for IP Telephony can discover the publisher Cisco Unified Communication Manager (CUCM) whose CallManager service is deactivated or stopped.

To configure the AXL access for Cisco:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Data Access Configuration**. This opens the NNM iSPI for IP Telephony Data Access Configuration form.
3. Click the **Cisco** tab.
4. Click the **AXL Access** tab.
5. In the **Add/Modify AXL access configuration for a cluster** section, specify the following details in the **Value** box for each of the following parameters:
 - **Tenant:** Select the name of the tenant. You can select the name of the tenant from the drop-down list.
 - **Cluster ID:** Type the cluster identifier. You can retrieve this information from the administration web page of the Cisco Unified Communications Manager.
 - **CM IP Address:** Type 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:** specifies the AXL user name to be used for invoking the AXL Web Services.
 - **AXL Password:** specifies the password associated with the user name specified.
6. Click **Add/Modify**.

The **Current Configurations** section lists the number of clusters configured for AXL access.

To delete an AXL access configuration:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Cisco** tab and then click the **AXL Access** tab.
2. Select the configuration from the **Current Configuration** section.
3. Click **Delete** to delete the AXL access configuration.

To modify an AXL access configuration:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Cisco** tab and then click the **AXL Access** tab.
2. Select the configuration from the **Current Configuration** section.
3. Click **Modify** to modify the AXL access configuration.
4. Modify the following details:
 - **CM IP Address**
 - **AXL User Name**
 - **AXL Password**

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.

Access the CDR Data

You must perform this configuration task if you want to use the CDR reporting feature. To monitor the phone MAC data, you must configure the NNM iSPI for IP Telephony to discover switches that are connected to phones.

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

Prerequisites

You must configure an FTP 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):
 - a. Set up an FTP server on the NNMi management server.
 - b. Create a user on the NNMi management server with the read/write access to the following location:

Windows: %NnmDataDir%\shared\ipt\IPTCiscoCDRCollection

UNIX/Linux: /var/opt/OV/shared/ipt/IPTCiscoCDRCollection

- c. Set up the home directory for the FTP server.

For Windows only. Configure the

%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection directory as the home directory of the FTP server.

For UNIX/Linux. Make sure that the / (root) directory is configured as the home directory of the FTP server

- d. 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.

- For an NNMi management server in an HA cluster:
 - a. Set up an FTP server on each NNMi management server in the HA cluster.
 - b. 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

UNIX/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.

- c. Set up the home directory for the FTP server.

For Windows only. Configure the <Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection directory as the home directory of the FTP server.

For UNIX/Linux. Make sure that the / (root) directory is configured as the home directory of the FTP server.

- d. 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 UNIX/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
 - *UNIX/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.

In the list of parameters, you must specify the FTP user credentials created in above.

For Directory Path, specify the complete path of the newly created directory if NNMi is installed on a UNIX/Linux server; specify only the name of the newly created directory if NNMi is installed on a Windows server.

For example, for NNMi on Linux, specify
/var/opt/OV/shared/ipt/IPTCiscoCDRCollection/.

For NNMi on Windows, specify /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):
 - a. Set up an FTP or SFTP server on the NNMi management server.
 - b. Create a user on the NNMi management server with the read/write access to the following location:

Windows: %NnmDataDir%\shared\ipt\IPTCiscoCDRCollection

UNIX/Linux: /var/opt/OV/shared/ipt/IPTCiscoCDRCollection

- c. Set up the home directory for the FTP or SFTP server.

For Windows only. Configure the
%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection directory as the home
directory of the FTP or SFTP server.

For UNIX/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:
 - a. Set up an FTP or SFTP server on each NNMi management server in the HA cluster.
 - b. 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

UNIX/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.

- c. Set up the home directory for the FTP or SFTP server.

For Windows only. Configure the <Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection directory as the home directory of the FTP or SFTP server.

For UNIX/Linux. Make sure that the / (root) directory is configured as the home directory of the FTP or SFTP server.

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 UNIX/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
 - *UNIX/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.

In the list of parameters, you must specify the FTP or SFTP user credentials created in above.

For Directory Path, specify the complete path of the newly created directory if NNMi is installed on a UNIX/Linux server; specify only the name of the newly created directory if NNMi is installed on a Windows server.

For example, for NNMi on Linux, specify
/var/opt/OV/shared/ipt/IPTCiscoCDRCollection/.

For NNMi on Windows, specify /IPTCiscoCDRCollection/.

Configure the NNM iSPI for IP Telephony to Access the CDR Data

To configure CDR access for a Cisco Unified Communications Manager cluster:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Data Access Configuration**. This opens the NNM iSPI for IP Telephony Data Access Configuration form.
3. Click the **Cisco** tab.
4. Click the **CDR Access** tab.
5. In the **Add/Modify Configuration for accessing CDR on Demand Web Service in Cisco Unified Communication Manager Clusters** section, specify the following details:
 - **Tenant**: specifies the name of the tenant. You can select the name of the tenant from the drop-down list.
 - **Cluster ID**: specifies the cluster identifier. You can retrieve this information from the administration web page of the Cisco Unified Communications Manager.
 - **CDR Polling Interval**: Specify 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.
6. Select **True** if you want the iSPI for IP Telephony to use the CDRonDemand Web Service to collect the CDR files.

If you select **False**, specify the complete path to the newly created directory in the CDR Files Download Path box. Cisco Unified Communications Manager deems 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, it is recommended 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.

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 Username**: Simple Object Access Protocol (SOAP) user name of the CDRonDemand WebService
 - **SOAP Password**: Password of the above user
 - **Port**: CDR on demand web service port
7. Click **Add/Modify**.

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:

Note: Skip these steps if you do not use CDRonDemand Web Service to collect CDR data from any of the Cisco Unified Communications Manager clusters.

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Cisco** tab, and then click the **CDR Access** tab.
2. Specify the following FTP details in the **(S)FTP server information to be used by iSPI for IP Telephony** section:
 - **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.
 - **Username**: A valid SFTP or FTP user name with write privileges on the NNM iSPI for IP Telephony server.
 - **Password**: The password for the SFTP or FTP user name specified.
 - **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**.

This procedure restarts the 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 iSPI for IP Telephony accesses the CDR data.

To configure FTP credentials to be used by CDRonDemand Web Service to send the CDR files to the NNM iSPI for IP Telephony:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Cisco** tab, and then click the **CDR Access** tab.

2. Specify the following FTP details in the **Configuring FTP username/password to be used by CDR on demand Web Services to send CDR files to the IPTSPI Server** section:
 - **FTP Username:** A valid FTP user name with write privileges on the iSPI for IP Telephony server.
 - **FTP Password:** The password for the FTP user name specified.
 - Select True or False for the Use FTP server FQDN instead of IP Address option.
3. Click **Apply**

This procedure restarts the 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 iSPI for IP Telephony accesses the CDR data.

The NNM iSPI for IP Telephony uses the following directory as the FTP or SFTP 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 delete the configuration for the CDRonDemand Web Service access for a Cisco Unified Communications Manager Cluster:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Cisco** tab and then click the **CDR Access** tab.
2. Select the CDR access configuration, which you want to delete, from the **Current Configurations** section.
3. Click **Delete**

This procedure restarts the iSPI for IP Telephony task that monitors the QOS/MOS for IP Telephony calls.

To modify the configuration for the CDRonDemand Web Service access for a Cisco Unified Communications Manager Cluster:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Cisco** tab and then click the **CDR Access** tab.
2. Select the CDR access configuration, which you want to modify, from the **Current Configurations** section.
3. Click **Modify**.
4. Modify the **CDR Polling Interval**. For best results, set this interval in the range of 2 minutes through 60 minutes.

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.

5. Select **True** for the **Is CDR onDemand WS Based Collection?** if you want the iSPI for IP Telephony to use the `CDRonDemand Web Service` to collect the CDR files.
6. Click **Add/Modify**.

This procedure restarts the iSPI for IP Telephony task that monitors the QOS/MOS for IP Telephony calls.

Access the Cisco Unified Communications Manager with SSH

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 NNM iSPI for IP Telephony Data Access Configuration page, click the **Cisco** tab and then click the **SSH Access** tab.
2. In the **Add/Modify SSH Configuration** section, provide the following details to configure the SSH access for the specific call manager:
 - **CM IP Address:** specify 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:** specify the type of SSH application to be used to collect the call details. The iSPI for IP Telephony uses the `CISCO_UCM_UCOS_DEFAULT` application by default.
 - **User Name:** specify the user name to be used to establish an SSH connection.
 - **Password:** specify the password to be used for the user name.
 - **Port:** specify the port number to be used for the SSH connection.
 - **Timeout:** specify the number of seconds to wait while attempting to execute a command before canceling the attempt.
 - **Host Key:** specify the SSH host key for the call manager.
3. Click **Add/Modify** to complete the configuration. The iSPI for IP Telephony lists the added configuration in the **Current Configuration** section.

To modify an existing SSH configuration:

1. Select an existing SSH configuration from the **Current Configuration** section.
2. Click **Modify**
3. Specify the required values for the configuration in the **Add/modify SSH Configuration** section
4. Click **Add/Modify** to complete the configuration.

To delete an existing configuration:

1. Select an SSH Configuration from the **Current Configuration** section
2. Click **Delete**. This deletes the selected configuration.

Configuring Data Access for Avaya

You can use the NNM iSPI for IP Telephony Data Access Configuration form to configure the CDR data access for Avaya.

To configure CDR access for Avaya:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Data Access Configuration**. This opens the NNM iSPI for IP Telephony Data Access Configuration form.
3. Click the **Avaya** tab.
4. Click the **CDR Access** tab.
5. In the **Add/Modify CDR access configuration** section, specify the following details in the **Value** box for each of the following parameters:
 - **CM IP Address:** specifies the IP address of the communication manager server from which the 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:** specifies 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.
- **Circuit ID Modified?:** Select **True** here 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 had specified *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 had specified *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 have selected **True** for Configured for Survivability option, you must provide the Secure File Transfer Protocol (SFTP) credentials to be used by the 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 have selected **False** for Configured for Survivability option, you must specify the following information to configure CDR data access using RSP:

- **CDR Port Number:** Type the port number that is configured on the Avaya CM for Call Detail Reports. 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 your network supports Network Address Translation (NAT) or Port Address Translation (PAT), you must specify the external IP address (public address) here.

6. Click **Add/Modify..**

The **Current Configurations** section lists the details of the communication managers configured for CDR access.

To delete an Avaya IP Telephony CDR access configuration:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Avaya** tab and then click the **CDR Access** tab.
2. Select the **CM IP Address** from the **Current Configurations** section.
3. Click **Delete** to delete the specified Avaya IPT CDR access configuration.

To modify an Avaya IP Telephony CDR access configuration:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Avaya** tab and then click the **CDR Access** tab.
2. Select the **CM IP Address** from the **Current Configurations** section.
3. Click **Modify** to modify the specified Avaya IPT CDR access configuration.
4. Specify the details listed in [Step 5](#).
5. Click **Add/Modify**.

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 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 iSPI for IP Telephony includes a sample customized CDR format specification file at the following location: `%NNM_DATA_DIR%/shared/ipt/conf/CustomizedCDRFormat.properties` where `%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.

To configure RTCP access for Avaya:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Data Access Configuration**. This opens the NNM iSPI for IP Telephony Data Access Configuration form.
3. Click the **Avaya** tab.
4. Click the **RTCP Reception** tab.
5. Specify the following details for the RTCP reception configuration:
 - **Enable Reception**: select this check box to enable the NNM iSPI for IP Telephony to receive and process the RTCP packets.
 - **Vendor**: specify the vendor name for the RTCP reception configuration.
 - **Sender Type**: specify the value that indicates the type of the sender.
 - **IP address on iSPI for IP Telephony system**: specify 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 this 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**: specify 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**: specify the port number on the iSPI for IP Telephony server where you want to receive RTCP packets from the Avaya end points controlled by this communication manager.

- **IP Address of the Communication Manager:** specify 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:** specify the remote IP address type of the Communications Manager.
- **Tenant:** specify the name of the tenant. You can select the name of the tenant from the drop-down list.
- **Enable Reporting:** select Enable Reporting 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 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 iSPI for IP Telephony server. For more information on partitioning of RTCP reception across different iSPI for IP Telephony regional manager instances in a GNM environment, see the iSPI for IP Telephony Deployment Guide.

6. Click **Add/Modify**.

To delete an RTCP reception configuration:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Avaya** tab and then click the **RTCP Reception** tab.
2. Select the configuration that you want to delete from **the Current Configurations** section.
3. Click **Delete** to delete the specified RTCP reception configuration.

To modify an Avaya IP Telephony RTCP reception configuration:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Avaya** tab and then click the **RTCP Reception** tab.
2. Select the configuration that you want to modify from **the Current Configurations** section.
3. Click **Modify** to modify the specified RTCP reception configuration.
4. Select or clear the Enable Reception and Enable Reporting check boxes.

Note: You cannot modify the other details.

5. Click **Add/Modify**.

Configuring SSH Access for Avaya

You must configure the required Secure Shell (SSH) access details using the Data Access Configuration form provided by the NNM iSPI for IP Telephony. 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 these servers as listed below:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Data Access Configuration**. This opens the NNM iSPI for IP Telephony Data Access Configuration form.
3. Click the **Avaya** tab.
4. Click the **SSH Access** tab.
5. Under the **Add/Modify SSH Configuration** section, specify the following details in the value box for each of the following parameters:
 - **CM IP Address**: specifies the IP address of the Avaya 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**: specifies the type of application used to access data on the primary communication manager server. The iSPI for IP Telephony currently supports only System Access Terminal (SAT) application. You cannot edit the value in this box.
 - **User Name**: specifies the SSH user name to log on to the primary communication manager server.
 - **Password**: specifies the password for the user name specified.
 - **Port Number**: specifies the port number on the primary communication manager server to which SSH connections can be established from the iSPI for IP Telephony server.
 - **Timeout**: specifies the number of seconds to wait while attempting to execute a command, before canceling the attempt and generating an error.
 - **Host Key**: specifies 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.
6. Click **Add/Modify**.

The **Current Configuration** section lists all the signaling servers configured for SSH access.

To delete an SSH access configuration:

1. On the **NNM iSPI for IP Telephony Data Access Configuration** page, click the **Avaya** tab.
2. Click the **SSH Access** tab.

3. Under the **Current Configuration** section, select the **CM IP address** of the SSH server that you want to delete.
4. Click **Delete** to delete the SSH access configuration.

To modify an SSH access configuration:

1. On the **NNM iSPI for IP Telephony Data Access Configuration** page, click the **Avaya** tab.
2. Click the **SSH Access** tab.
3. Under the **Current Configuration** section, select the **CM IP address** of the SSH server that you want to modify.
4. Click **Modify** to modify the SSH access configuration.
5. Specify the details listed in [step 5](#) of the Configuring SSH Access for Avaya section.
6. Click **Add/Modify**.

Configuring Data Access for Nortel

You can use the NNM iSPI for IP Telephony Data Access Configuration form to configure data access for Nortel.

You can also use this form to delete the data access points:

To configure signaling server SSH access:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Data Access Configuration**. This opens the NNM iSPI for IP Telephony Data Access Configuration form.
3. Click the **Nortel** tab.
4. On the Signaling Server SSH Access tab page, under the **Add/Modify Signaling Server SSH Login Access Configuration** section, specify the following details in the **Value** box for each of the following parameters:
 - **ELAN IP Address**: specify the Embedded LAN (ELAN) IP address of the signaling server.
 - **TLAN IP Address**: specify the Telephony LAN (TLAN) IP address of the signaling server.
 - **Auto accept Host Key?**: specify if the host key must be accepted automatically for the signaling server. Select **True** to enable this feature.
 - **Host Key Algorithm?**: specify the host key algorithm. You can select one of the following algorithms:
 - **ssh-rsa**: specify authentication using the ssh-rsa key pair.
 - **ssh-dss**: specify authentication using the ssh-dss key pair.
 - **Host Key HexFingerprint**: specify the host key fingerprint in hexadecimal format.
 - **User Name**: specify the user name to log on to the signaling server.
 - **Password**: specify the password for the user name specified.

- **PEM File Location:** specifies 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:** specifies the password for the PEM file if the file is encrypted.
- **Call Server Username:** specifies the user name to log on to the call server of the signaling server.
- **Call Server Password:** specifies the password for the user name specified.

5. Click **Add/Modify**.

The **Current Configurations** section lists all the signaling servers configured for SSH access.

To delete a Signaling Server SSH access configuration:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Nortel** tab.
2. Select the ELAN IP address of the signaling server that you want to delete from the **Current Configuration** section.
3. Click **Delete** to delete the .Signaling Server SSH access configuration.

To modify a Signaling Server SSH access configuration:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Nortel** tab.
2. Select the ELAN IP address of the signaling server that you want to delete from the **Current Configuration** section.
3. Click **Modify** to modify the .Signaling Server SSH access configuration.
4. Specify the details listed in step 4 of the ["Configuring Data Access for Nortel" \(on page 262\)](#) section.
5. Click **Add/Modify**.

Extracting a Host Key for the Avaya Communication Manager and Cisco Unified Communications Manager

To extract an RSA level 2 host key for Avaya Communication Manager (CM) or Cisco Unified Communications Manager (CUCM), follow these steps:

- **On UNIX/Linux**

1. Make sure that no trusted host key is stored for the CM or CUCM 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.

- b. Delete the entry that corresponds to the IP address of the CM or CUCM. For example, if the IP address of your CM or CUCM is 192.168.16.17, the host key that corresponds to the CM or CUCM may look like this:

```
192.168.16.17 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEARC1tF99fLtDQxAPoG+JLGnT10WWEtInB2w4SL3+Om6je9deYr8k
```

2. Run an `ssh` command to the IP address of the remote CM or CUCM 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
established.
```

```
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.

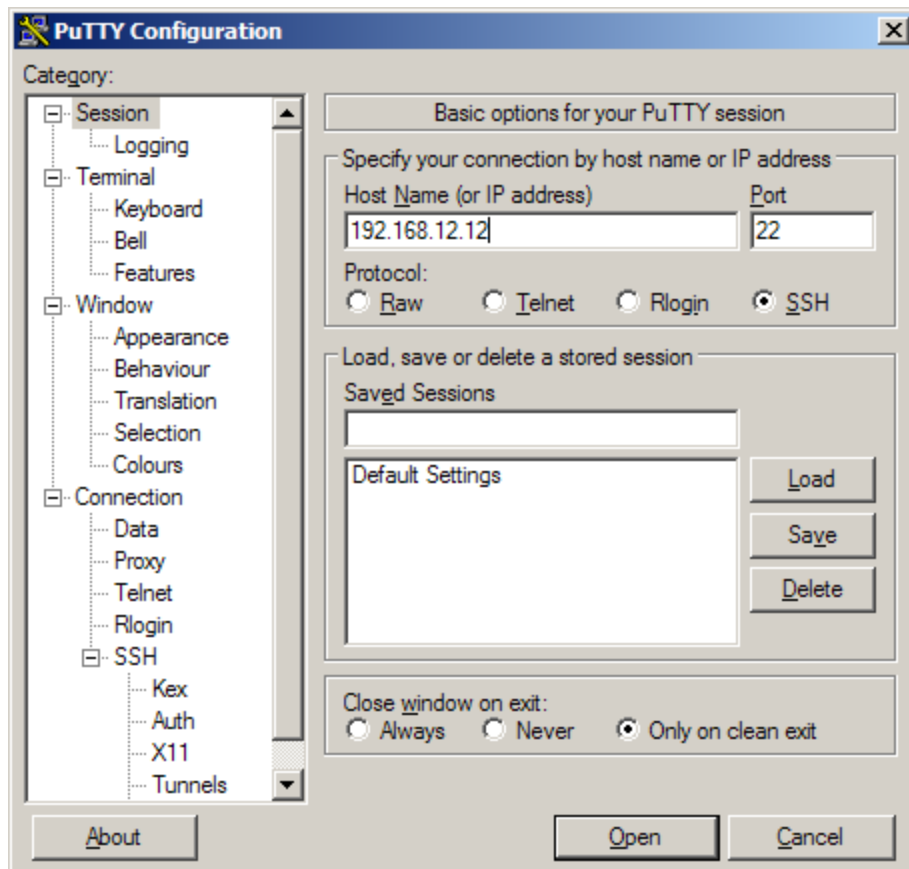
- **On Windows**

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 or CUCM using the PuTTY application, follow these steps:

Note: The following steps are for extracting the host key using the PuTTY application, but you can use any other similar application.

1. Open the PuTTY application and type the host name or IP address of the CM or CUCM under 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.

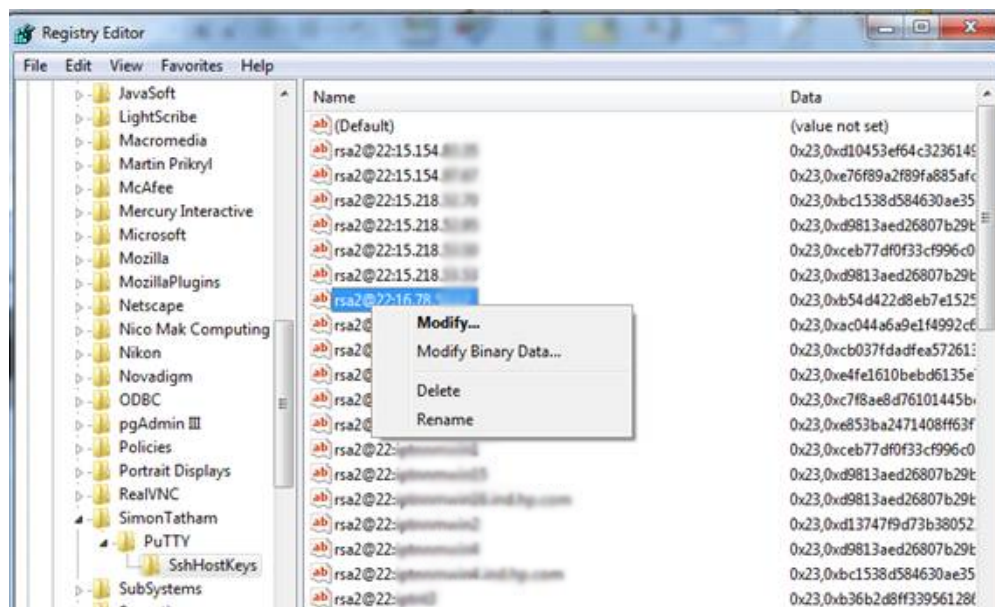
Note: If the pop-up window does not open, go to [step 5](#).

5. If the pop-up window mentioned in [step 4](#) does not open, the host key for the IP address of the CM or CUCM is already cached in the registry by PuTTY in a previous session. In this scenario, you must clear the registry entry and perform [step 1](#) to [step 4](#) again.

To clear the registry entry:

- 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 or CUCM.
 - c. Click **Delete**.
6. Repeat [step 1](#) to [step 4](#).

Configuring Monitoring Tasks

Click the **Monitoring Configuration** link on the IP Telephony Configurations page to specify the options to configure monitoring for IP Telephony devices. You can specify the polling configuration options for the Cisco, Avaya, and Nortel IP Telephony devices. Click the following links to know more about changing monitoring configuration for IP Telephony devices:

- ["Configuring Monitoring Tasks Related to Cisco IP Telephony" \(on page 267\)](#)
- ["Configuring Monitoring for Avaya IP Telephony Devices" \(on page 276\)](#)
- ["Configuring Monitoring Tasks for Nortel IP Telephony" \(on page 285\)](#)

Configuring Monitoring Tasks Related to Cisco IP Telephony

Click the **Cisco** tab to perform the following monitoring configuration tasks:

- [Configure the QOS and MOS Monitoring Threshold Values for Cisco](#)
- [Configure the Call Termination Cause Monitoring Codes to be Monitored](#)
- [Configuration for monitoring Registration State & Controller Association of IP Phones](#)
- [Configure the Monitoring of Call Managers](#)
- [Configure the Monitoring of Voice Gateway Channels](#)
- [Configure the Monitoring of Voice Gateway Interfaces](#)
- [Configure the Monitoring of Gatekeepers](#)
- [Configure the Monitoring of Call Manager Voice Mail Devices](#)
- [Configuration for Survivable Remote Site Telephony \(SRST\) monitoring](#)
- [Configure the Monitoring of License Consumption for Unity Devices and Unity Connection Servers](#)

Configuring the QOS and MOS Monitoring Threshold Values for Cisco

The Thresholds for QOS/MOS Monitoring tab page allows 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:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Cisco** tab.
4. Click the **Call Monitoring** tab.

5. Click the **Thresholds for QOS/MOS Monitoring** tab. This opens the Thresholds for QOS/MOS Monitoring tab page.
6. Specify threshold values for the following QOS and MOS monitoring parameters:

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.

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, for a 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 ranges from 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.

¹To disable the monitoring, specify **-1**.

²To disable the monitoring, specify **0.0**.

7. Click **Apply**. This restarts the Cisco IP telephony QOS and MOS monitoring process.

Configuring Cluster-Specific QOS and MOS Monitoring Threshold Values

The Thresholds for QOS/MOS Monitoring tab page provides the **Add Cluster Specific QOS Configuration** section that you can use to configure QOS and MOS monitoring threshold values for specific clusters of your choice. After you specify threshold values specific to a cluster, the iSPI for IP Telephony uses these threshold values for the specific cluster instead of the threshold values you specified in the *Thresholds for QOS/MOS Monitoring* section. After you configure the threshold values for a cluster, the iSPI for IP Telephony lists the cluster-specific threshold values in the **Current Configuration** section.

To configure cluster-specific QOS and MOS Monitoring Threshold Values:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Cisco** tab.
4. Click the **Call Monitoring** tab.

5. Click the **Thresholds for QOS/MOS Monitoring** tab. This opens the Thresholds for QOS/MOS Monitoring tab page.
6. Select the name of the tenant from the **Tenant** drop-down list present in the **Add Cluster Specific QOS Configuration** section.
7. Select the required cluster for which you want to configure threshold values from the **Cluster ID** list box.
8. Specify the required QOS and MOS monitoring threshold values listed for the parameters listed.
9. Click **Add/Modify**. This adds the configuration for the cluster in the **Current Configuration** section.

To modify cluster-specific QOS and MOS Monitoring Threshold Values:

1. Select the cluster specific configuration that you want to modify, from the **Current Configuration** section.
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 required and click **Add/Modify**. This updates the cluster specific configuration with the new values.

To delete cluster-specific QOS and MOS Monitoring Threshold Values:

1. Select the cluster specific configuration that you want to delete, from the **Current Configuration** section.
2. Click **Delete**. This deletes the cluster-specific threshold values for the cluster. After removing the cluster-specific threshold value configuration, the iSPI for IP Telephony uses the values you provided in the *Thresholds for QOS/MOS Monitoring* section.

Configure Call Termination Cause Codes to be Monitored




You can configure the 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 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:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.

2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
 3. Click the **Cisco** tab.
 4. Click the **Call Monitoring** tab. You might have to scroll the tab listing using the scroll button () to reveal this tab.
 5. Click the **Call Termination Cause Monitoring** tab.
 6. 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 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 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).
7. Click **Apply** to complete this configuration.

Configure the Monitoring for Registration State and Call Manager Association of IP Phones

After the NNM iSPI for IP Telephony discovers the available Cisco IP Phones on the network, the monitoring for the registration state and controller association of IP Phones occur with the default monitoring frequency. You can modify the default frequency using the NNM iSPI for IP Telephony Polling Configuration form.

To configure the polling for registration state and controller association of IP Phones:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration**. The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Cisco** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **IP Phones** tab to specify the monitoring options for the IP Phones.
5. In the **Monitoring IP Phone Registration State Changes and IP Phone to Call Manager Associations** section, specify the following details:
 - **Enable Polling** Select this option to enable the polling for IP Phones.
 - **Interval**: Specify the period (in seconds). The default frequency is 900 seconds.

Note: Do not specify a value less than 900 seconds. However, you can specify a larger period for this monitoring task. Also note that, this monitoring task is very resource consuming as it collects all the IP Phone information from the Clusters.

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.

6. Click **Apply Changes**.

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 cluster that includes the IP phones.

To specify the list of IP phones for registration state change incident generation:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration**. The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Cisco** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **IP Phones**.
5. Specify the following details in the **Add/Modify Filters for IP Phones for which Registration State change Incidents are to be generated** section:
 - a. In the **Tenant** drop-down list, select the name of the tenant that contains the IP phones, for which the registration state change incidents are to be generated.
 - b. Specify the ID of the cluster in the **Cluster ID** box. This ID specifies the cluster that includes the list of phones for which the registration state change incident must be generated.
 - c. In the **Filter** section, specify the extension range to be included. See the section ["Specifying the List of IP Phones for Registration State Change Incident Generation" \(on page 271\)](#) for more information about specifying extension ranges.
6. 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. You can select a configuration and click **Delete** to delete the configuration.

Configure the Monitoring of Call Managers

After the NNM iSPI for IP Telephony discovers the available Cisco CallManagers on the network, the monitoring of the Cisco CallManager servers occur with the default monitoring frequency. You can modify the frequency using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the polling for Cisco Call Managers:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Cisco** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Call Managers** tab to specify the monitoring options for the call managers.
5. In the **Configuration for CallManager Service State monitoring** section, specify the following details:
 - **Enable Polling:** Select this option to monitor the state of the call managers.
 - **Interval:** Specify the frequency (in seconds) to poll the state of the call managers. The default frequency is 300 seconds.
6. Click **Apply Changes**.

Configure the Monitoring of Voice Gateway Channels

With the IP Telephony Configurations form, you can set the monitoring frequency to poll the *usage* and *operational* states of discovered voice gateway channels. You can modify the default monitoring frequency using the NNM iSPI for IP Telephony Polling Configuration form.

To configure the time that the NNM iSPI for IP Telephony waits for before declaring that a channel is Idle:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Voice Gateway Channel** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for Voice Gateway Channel usage Monitoring (Wait time to declare idle)** section, specify the following details:
 - **Wait before declaring Idle:** Select this option to specify that the voice gateway channel must be declared idle only after waiting for the specified time.
 - **Time to wait before declaring idle:** Specify the interval (in seconds) for which the iSPI must wait for before marking the usage state of a channel to Idle. The default interval is 300 seconds. For example if you specify 300 seconds as the waiting time and period of the usage state monitoring for channels is 150 seconds, then, during the monitoring of usage state for channels, if the NNM iSPI for IP Telephony finds the usage state to be Idle, the iSPI for IP Telephony waits for 2 subsequent periodic usage state monitoring cycles to find the usage state to be Idle and then declare the usage state to be Idle. Note that if the usage state is detected to be anything other than Idle, then the waiting period is not applicable or the waiting period is abandoned.
5. Click **Apply Changes**.

To configure the monitoring for voice gateway channel usage state:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Voice Gateway Channel** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for Voice Gateway Channel Usage State Monitoring** section, specify the following details:
 - **Enable Polling:** Select this option to monitor the usage states of voice gateway channels.
 - **Interval:** Specify the interval (in seconds) to poll the voice gateway channels. The default interval is 300 seconds.
5. Click **Apply Changes**

Configure the Monitoring of Voice Gateway Interfaces

With the NNM iSPI for IP Telephony Configuration form, you can set the monitoring frequency to poll the states of discovered voice gateway interfaces. You can modify the default frequency using the NNM iSPI for IP Telephony Monitoring Configuration form. In addition, this form helps you set the options to monitor the registration state of a voice gateway interface.

To configure the monitoring for the operational state of voice gateway interfaces:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Voice Gateway Interface(s)** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for Voice Gateway Interface Operational State monitoring** section, specify the following details:
 - **Enable Polling:** Select this option to poll the operational states of voice gateway interfaces.
 - **Interval:** Specify the interval (in seconds) to monitor the operational states of voice gateway interfaces. The default interval is 180 seconds.
5. Click **Apply Changes**.

To configure the monitoring for the registration state and controller association of voice gateway interfaces:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Voice Gateway Interface(s)** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.

4. In the **Configuration for Registration State & Controller-association of Voice Gateway Interfaces monitoring (MGCP Only)** section, specify the following details:
 - **Enable Polling** Select this option to monitor the registration state and controller association of voice gateway interfaces.
 - **Interval:** Specify the interval (in seconds) to monitor the registration states and controller association of circuit-switched interfaces. The default interval is 300 seconds..
5. Click **Apply Changes**.

Configure the Monitoring of Gatekeepers

In the Gatekeepers view, the NNM iSPI for IP Telephony lists all the discovered Cisco gatekeeper devices with the number of endpoints associated with every gatekeeper device. You can configure the frequency to monitor the discovered Cisco gatekeepers to read the number of associated endpoints. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Polling Configuration form.

To configure the monitoring of count of endpoints registered with the Gatekeeper:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Gatekeepers** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for monitoring Gatekeepers' count of registered endpoints** section, specify the following details:
 - **Enable Polling:** Select this option to collect the number of endpoints registered with every gatekeeper.
 - **Interval:** Specify the frequency (in seconds) to monitor the number of endpoints registered with every gatekeeper. The default interval is 300 seconds.
5. Click **Apply Changes**.

Configuration for monitoring Registration State of Gatekeeper controlled Inter Cluster Trunks:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **GateKeeper** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for monitoring Registration State of Gatekeeper controlled Inter Cluster Trunks** section, specify the following details:
 - **Enable Polling:** Select this option to monitor the registration states of Cisco gatekeeper-controlled intercluster trunks.
 - **Interval:** Specify the interval (in seconds) to monitor the registration states of Cisco gatekeeper-controlled intercluster trunks. The default interval is 300 seconds.
5. Click **Apply Changes**.

Configure the Monitoring of Call Manager Voice Mail Devices

In the **Voice Mail Devices** tab on the Cisco Call Controller detail view, the NNM iSPI for IP Telephony lists all the discovered Cisco Call Manager Voice Mail devices known to the selected Call Manager. You can configure the default interval to monitor the registration state of the Call Manager Voice Mail devices. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Monitoring Configuration form.

Configuration for Registration State of Call Manager Voice Mail Devices monitoring:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration...** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Call Manager Voice Mail Devices** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for Registration State of Voice Mail (VM) Devices monitoring** section, specify the following details:
 - **Enable Polling**: Select this option to monitor the state of the discovered VM devices.
 - **Interval**: Specify the interval (in seconds) to monitor the state of the discovered VM devices. The default interval is 300 seconds.
5. Click **Apply Changes**.

Configuration for Survivable Remote Site Telephony (SRST) Monitoring

After the NNM iSPI for IP Telephony discovers the available Cisco SRST routers on the network, the monitoring occurs with the default monitoring frequency. You can modify the default monitoring frequency using the NNM iSPI for IP Telephony Monitoring Configuration form.

To change Configuration for Survivable Remote Site Telephony (SRST) State Monitoring:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration...** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **SRSTs** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for Survivable Remote Site Telephony (SRST) State Monitoring** section, specify the following details:
 - **Enable Polling**: Select this option to monitor the states of SRST routers.
 - **Interval**: Specify the frequency (in seconds) to monitor the states the routers. The default value is 300 seconds.
5. Click **Apply Changes**.

Configure the Monitoring of License Consumption for Unity Devices and Unity Connection Servers

You can configure the monitoring of the license points consumed by the Cisco Unity devices and Unity Connection servers along with monitoring of the port utilization.

To change Configuration for monitoring the license consumption for Cisco Unity devices and connection servers:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Unity and Unity Connection** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for License consumption and port utilization monitoring** section, specify the following details:
 - **Enable Polling:** Select this option to monitor the license points consumed.
 - **Interval:** Specify the frequency (in seconds) to monitor the states the routers. The default value is 300 seconds.
5. Click **Apply Changes**.

Configuring Monitoring for Avaya IP Telephony Devices

Click the **Avaya** tab to specify the monitoring options for the following Avaya IP Telephony device states and statistics:

- [CLAN and IP Phone Association](#)
- [IP Phones](#)
- [Media Processors](#)
- [IP Server Interfaces](#)
- [IP Network Regions](#)
- [External Call Controllers](#)
- [Survivable Servers](#)
- [Media Gateways](#)
- [Route Pattern](#)
- [Trunk Group Usage and Trunk Member State](#)
- [Port Network Load Statistics](#)
- [Processor Occupancy Statistics](#)

Configure the Monitoring for CLAN and IP Phone Association

The NNM iSPI for IP Telephony continuously tracks the association between the Avaya IP Phones and the Avaya Control LAN (CLAN) on the network. You can configure the monitoring interval for this monitoring task using the NNM iSPI for IP Telephony Monitoring Configuration form.

If your network supports Network Address Translation (NAT) protocol or Port Address Translation (PAT) protocol, you must map the external IP address and the internal IP address of all Avaya CLANs and Avaya IP phones using Overlapping Address Mapping form of NNMi. If you do not do this mapping, the CLAN and IP phones association polling may not take place.

To configure the monitoring for CLAN and Avaya IP Phone association:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **CLAN and IP Phone Association** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
5. In the **Configuration for CLAN and IP Phone Association monitoring** section, specify the following details:
 - **Enable Polling:** Select this option to monitor the CLAN to find the CLAN and IP Phone association.
 - **Interval:** Specify the interval (in seconds) to monitor the CLAN. The default value is 300 seconds.
6. Click **Apply Changes**.

Configure the Monitoring for IP Phones

The NNM iSPI for IP Telephony continuously monitors the registration state of the Avaya IP Phones on your network. You can configure the monitoring interval for this monitoring task using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring for Avaya IP Phones:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **IP Phones** tab.
5. In the **Configuration for IP Phones Registration State monitoring** section, specify the following details:

- **Enable Polling:** Select this option to monitor the Avaya IP phones.
- **Interval:** Specify the interval (in seconds) to monitor the Avaya IP Phones. The default value is 300 seconds.

6. Click **Apply Changes**.

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 Communication Manager that includes the IP phones.

To specify the list of IP phones for registration state change incident generation, do as follows:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration**. The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **IP Phones**.
5. Specify the following details in the **Add/Modify Filters for IP Phones for which Registration State change Incidents are to be generated** section:
 - a. Specify the IP address of the communication manager in the **CM IP Address** box. This IP address specifies the communication manager IP address that includes the list of phones for which the registration state change incident must be generated .
 - b. In the **Filter** section, specify the extension range to be included. See the section ["Configure the Monitoring for IP Phones" \(on page 277\)](#) for more information about specifying extension ranges.
6. 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. You can select a CM IP address and click **Delete** to delete the existing configuration.

Configure the Monitoring for Media Processors

The NNM iSPI for IP Telephony continuously monitors the various states of Avaya Media Processors (MedPros, Prowlers) on the network. The monitoring for these states occur with the default monitoring interval. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring for media processors:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.

2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Media Processors** tab to specify the monitoring options for the media processors.
5. In the **Configuration for monitoring the various states of Media Processors** section, specify the following details:
 - **Enable Polling**: Select this option to enable the monitoring for media processors.
 - **Interval**: Specify the monitoring interval (in seconds). The default interval is 300 seconds.
6. Click **Apply Changes**.

Configure the Monitoring for IP Server Interfaces

The NNM iSPI for IP Telephony continuously monitors the various states of Avaya IP Server Interfaces (IPSI) on the network. The monitoring of these states occur with the default monitoring interval. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring for Avaya IP server interfaces:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **IP Server Interfaces** tab to specify the monitoring interval for the IP server interfaces.
5. In the **Configuration for monitoring various states of the IP Server Interfaces (IPSI)** section, specify the following details:
 - **Enable Polling**: Select this option to monitor the Avaya IP server interface objects.
 - **Interval**: Specify the monitoring interval (in seconds) to monitor the IP server interfaces. The default interval is 300 seconds.
6. Click **Apply Changes**.

Configure the Monitoring for IP Network Regions

The NNM iSPI for IP Telephony continuously monitors the following details for each IP Network Region configured on the Avaya Communications Manager server:

- The state of health for the connectivity of the IP Network Region with all the other logically connected IP Network Regions.
- The hourly DSP and CODEC usage and the related summary for DSP and CODEC resources deployed in the Network Region.

The monitoring for IP Network Regions occur with the default monitoring interval. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring for Avaya IP network regions:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **IP Network Regions** tab to specify the monitoring options for the IP Network Regions.
5. In the **Configuration for monitoring DSP, Codec Summaries, and Inter Region Connection States for IP Network Regions** section, specify the following details:
 - **Enable Polling**: Select this option to enable the monitoring for IP Network Regions.
 - **Interval**: Specify the monitoring interval (in seconds). The default interval is 900 seconds.
6. Click **Apply Changes**.

Configure the State Monitoring for the Duplex Primary Servers

The NNM iSPI for IP Telephony continuously monitors the state (Active/Standby) of the paired Avaya primary servers on the network. The monitoring to determine the states of such duplex paired primary servers occur with the default monitoring interval. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring for Avaya primary servers:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Primary Servers** tab to specify the monitoring interval for the primary server.
5. In the **Configuration for monitoring the State of Duplex Primary Servers** section, specify the following details:
 - **Enable Polling**: Select this option to enable monitoring of the primary server.
 - **Interval**: Specify the interval (in seconds) to monitor the primary server. The default value is 300 seconds.
6. Click **Apply Changes**.

Configure the State Monitoring for Survivable Servers

The NNM iSPI for IP Telephony Continuously monitors 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 monitoring to determine the state of the survivable servers occur with the default monitoring interval. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the state monitoring for survivable servers:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Survivable Servers** tab to specify the monitoring interval for the survivable servers.
5. In the **Configuration for Survivable Server State monitoring** section, specify the following details:
 - **Enable Polling:** Select this option to enable monitoring for the survivable server.
 - **Interval:** Specify the interval (in seconds) to monitor the survivable server. The default value is 300 seconds.
6. Click **Apply Changes**.

Configure the Monitoring for Media Gateways

After the NNM iSPI for IP Telephony discovers the available Avaya media gateways in the network, the monitoring to determine the state of the media gateways occur with the default monitoring interval. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring for media gateway state:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Media Gateways** tab to specify the monitoring interval for the media gateway.
5. In the **Configuration for monitoring the Media Gateway States** section, specify the following details:
 - **Enable Polling:** Select this option to monitor the media gateways.
 - **Interval:** Specify the interval (in seconds) to monitor the media gateways. The default value is 300 seconds.
6. Click **Apply Changes**.

To configure the monitoring for media gateway module state:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Media Gateways** tab to specify the monitoring interval for the media gateway.

5. In the **Configuration for monitoring the Media Gateway Module States** section, specify the following details:
 - **Enable Polling:** Set this option to monitor the media gateway modules.
 - **Interval** Specify the interval (in seconds) to monitor the media gateway modules. The default value is 300 seconds.

6. Click **Apply Changes**.

To configure the monitoring for media gateway DSP Core state:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Media Gateways** tab to specify the monitoring interval for the media gateway.
5. In the **Configuration for monitoring the Media Gateway VOIP Engines States** section, specify the following details:
 - **Enable Polling:** Set this option to monitor the media gateway DSP cores.
 - **Interval:** Specify the interval (in seconds) to monitor the media gateway VOIP engine state. The default value is 300 seconds.
6. Click **Apply Changes**.

To configure the monitoring for media gateway VOIP engine state:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Media Gateway** tab to specify the monitoring interval for the media gateway.
5. In the **Configuration for monitoring the Media Gateway DSP Core States** section, specify the following details:
 - **Enable Polling:** Set this option to monitor the media gateway DSP cores.
 - **Interval:** Specify the interval (in seconds) to monitor the media gateway DSP core state. The default value is 300 seconds.
6. Click **Apply Changes**.

Configure the Monitoring for Route Pattern Usage Metrics

You can configure the monitoring for the route pattern usage metrics using the NNM iSPI for IP Telephony Configuration form.

To configure the monitoring for Avaya route pattern usage metrics:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Route Pattern** tab to specify the monitoring options for the usage metrics of route patterns.
5. In the **Configuration for monitoring Route Pattern Usage Metrics** section, specify the following details:
 - **Enable Polling**: Select this option to enable polling of route pattern usage metrics.
 - **Interval**: Specify the monitoring duration for the route patterns (in seconds). The default interval is 1800 seconds.
6. Click **Apply Changes**.

Configure the Monitoring for Trunk Groups

You can use the NNM iSPI for IP Telephony Configuration form to configure the monitoring for trunk group usage metrics and the trunk member state.

To configure the monitoring for trunk group usage metrics:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Trunk Groups** tab to specify the monitoring options for the trunk group usage metrics.
5. In the **Configuration for monitoring Trunk Group Usage Metrics** section, specify the following details:
 - **Enable Polling**: Select this option to enable monitoring of trunk group usage metrics.
 - **Interval**: Specify the trunk group monitoring interval as required (in seconds). The default interval is 1800 seconds.
6. Click **Apply Changes**.

To configure the monitoring for trunk member state:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Trunk Groups** tab to specify the monitoring options for the trunk group usage metrics.

5. In the **Configuration for monitoring States of Trunk Group Members and Signaling Groups** section, specify the following details:
 - **Enable Polling:** Select this option to enable monitoring of the trunk member state.
 - **Interval:** Specify the trunk member state monitoring interval as required (in seconds). The default interval is 600 seconds.
6. Click **Apply Changes**.

Configure the Monitoring for Port Network Load Statistics

After the NNM iSPI for IP Telephony discovers the available port networks in the network, the monitoring to determine the port network load statistics occur with the default monitoring interval. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring for port network load statistics:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Port Network Load Statistics** tab to specify the monitoring interval for the port network load statistics.
5. In the **Configuration for Port Network Load Statistics Monitoring** section, specify the following details:
 - **Enable Polling:** Select this option to monitor the media gateways.
 - **Interval:** Specify the interval (in seconds) to monitor the media gateways. The default value is 120 seconds.
6. Click **Apply Changes**.

Configure the Monitoring for Processor Occupancy Statistics

After the NNM iSPI for IP Telephony discovers the available Avaya communications managers in the network, the monitoring to determine the processor occupancy statistics occur with the default monitoring interval. You can modify the default monitoring interval using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring for processor occupancy statistics:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Avaya** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **Processor Occupancy Statistics** tab to specify the monitoring interval for the processor occupancy statistics.

5. In the **Configuration for Processor Occupancy Statistics Monitoring** section, specify the following details:
 - **Enable Polling:** Select this option to monitor the media gateways.
 - **Interval:** Specify the interval (in seconds) to monitor the media gateways. The default value is 1800 seconds.
6. Click **Apply Changes**.

Configuring Monitoring Tasks for Nortel IP Telephony

Click the **Nortel** tab to specify the monitoring options for the following Nortel IP Telephony monitoring tasks:

- [QoS Zones](#)
- [IP Phones](#)

Configuring QoS Zones Monitoring

The NNM iSPI for IP Telephony monitors the various QoS-related measurements in the Nortel QoS Zones. The NNM iSPI for IP Telephony monitors the QoS metrics for all the configured QoS zones on discovered Nortel Signaling Servers. You can modify the default monitoring interval for this monitoring using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring threshold values for QoS Zones:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Nortel** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **QOS Zones** tab to specify the monitoring parameters for the QoS zone threshold.
5. In the **Configuration for QOS Zones monitoring** section, specify the following details:
 - **Enable Polling:** Select this option if you want to generate incidents based on the values of QoS metrics that are configured with the Nortel Signaling Server.
 - **Interval:** Specify the interval (in seconds) to monitor the Nortel Signaling Sever to collect the details of QoS metrics. The default value is 300 seconds.
6. Click **Apply Changes**.

Configure the Monitoring of IP Phones

The iSPI for IP Telephony continuously monitors the registration state of Nortel IP Phones on the network. The monitoring of the IP Phones occur with the default frequency. You can modify the default frequency using the NNM iSPI for IP Telephony Monitoring Configuration form.

To configure the monitoring for IP Phones:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration form opens.

2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Nortel** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **IP Phones** tab to specify the monitoring options for the IP Phones.
5. In the **Configuration for IP Phones Registration State monitoring** section, specify the following details:
 - **Enable Polling**: Select this option to monitor the registration state of the IP Phones.
 - **Interval**: Specify the interval (in seconds) to monitor the registration state of the IP Phones. The default interval is 1800 seconds.
6. Click **Apply Changes**.

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, do as follows:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration**. The NNM iSPI for IP Telephony configuration form opens.
2. Click **Monitoring Configuration**. This opens the NNM iSPI for IP Telephony Monitoring Configuration form.
3. Click the **Nortel** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. Click the **IP Phones**.
5. Specify the following details in the **Add/Modify Filters for IP Phones for which Registration State change Incidents are to be generated** section:
 - a. Specify the IP address of the Call Server in the **CS IP Address** box. 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 .
 - b. In the **Filter** section, specify the extension range to be included. See the section ["Configure the Monitoring of IP Phones" \(on page 285\)](#) for more information about specifying extension ranges.
6. 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 CS IP address from the list and click **Modify** to modify the existing configuration. You can select a CS IP Address click **Delete** to delete the existing configuration.

Reporting Configuration

You cannot enable Cisco or Avaya CDR reporting by the iSPI for IP Telephony till you install the iSPI Performance for Metrics. Ensure that you have a valid license for the iSPI Performance for Metrics on the NNMi server in your deployment environment before attempting to enable CDR

reporting. After enabling CDR reporting, if the NNM iSPI for IP Telephony detects an expired or invalid license during runtime for the iSPI Performance for Metrics on the NNMi server, the iSPI for IP Telephony stops processing and analyzing the CDR data obtained from Cisco Unified Communications Manager Clusters or the Avaya Communications Manager servers.

To access the Reporting Configuration form:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.

Configure Cisco IP Telephony CDR-based Reporting

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable CDR reporting for Cisco.

To configure Cisco CDR reporting:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Cisco** tab.
4. Click the **Reports Using CDR Data** tab. This opens the **Reports Using CDR Data** section.
5. Select **Enable Reporting**
6. Specify the number of processed calls to be sent to NPS or the Global Manager in an instance in the **No. of Calls to Write** box. The default value is 5000 for this attribute.
7. Select the **Calling and Called party Numbers in Reports** option to display the calling party number and the called party numbers in the Call Details reports.
8. Select the **Forward to Global Manager** option 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.
9. 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:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Cisco** tab.

4. Click the **B-Channel Activity Reports** tab. This opens the **B-Channel Activity Reports** section.
5. Select **Enable Reporting**.
6. 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 Media Access Control (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 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:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Cisco** tab.
4. Click the **Phone MAC Report** tab. This opens the **Phone MAC Reports** section.
5. Select **Enable Reporting**.
6. Specify the name of the configuration file that contains the comma-separated list of access switch IP addresses in the **Access Switches** box. This step 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`
7. Select the **Forward to Global Manager** option 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.
8. 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.lock` extension name in the file name.

- `ipt_server_name`: indicates the name of the 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:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.

2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Cisco** tab.
4. Click the **Voice Mail Report** tab. This opens the **Voice Mail Reports** section.
5. Select **Enable Reporting**.
6. Click **Apply Changes**.

Configure Avaya IP Telephony Reporting

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable CDR reporting for Avaya.

To configure Avaya CDR reporting:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Avaya** tab.
4. Click the **Reports Using CDR Data** tab. This displays the **Reports Using CDR Data** section.
5. Select **Enable Reporting** to enable Avaya CDR reporting.
6. Specify the number of processed calls to be sent to NPS or the Global Manager in an instance in the **No. of Calls to Write** box. The default value is 5000 for this attribute.
7. Select the **Calling and Called party Numbers in Reports** option to display the calling party number and the called party numbers in the Call Details reports.
8. Select the **Forward to Global Manager** option 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.
9. Click **Apply Changes**.

Enabling Trunk Activity Reports

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable trunk activity reports.

To configure trunk activity reporting:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Avaya** tab.
4. Click the **Trunk Activity Report** tab. This opens the **Trunk Activity Report** section.

5. Select **Enable Reporting**.
6. Click **Apply Changes**.

Enabling Trunk Group Usage Reports

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable trunk group usage reports.

To configure trunk group usage reporting:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Avaya** tab.
4. Click the **Trunk Group Usage Report** tab. This opens the **Trunk Group Usage Report** section.
5. Select **Enable Reporting**.
6. Click **Apply Changes**.

Enabling Processor Occupancy Summary Reports

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable processor occupancy summary reports.

To configure processor occupancy summary reporting:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Avaya** tab.
4. Click the **Processor Occupancy Summary Report** tab. This opens the **Processor Occupancy Summary Report** section.
5. Select **Enable Reporting**.
6. Click **Apply Changes**.

Enabling Port Network Load Reports

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable port network load reports.

To configure port network load reporting:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.

2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Avaya** tab.
4. Click the **Port Network Load Report** tab. This opens the **Port Network Load Report** section.
5. Select **Enable Reporting**.
6. 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 Media Access Control (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 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:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Avaya** tab.
4. Click the **Phone MAC Report** tab. This opens the **Phone MAC Reports** section.
5. Select **Enable Reporting**.
6. Specify the name of the configuration file that contains the comma-separated list of access switch IP addresses in the **Access Switches** box. This step 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`
7. Select the **Forward to Global Manager** option 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.
8. 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 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 IP Network Region DSP/Codec Summary Report

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable IP network region DSP/Codec summary reports.

To configure IP network region DSP/Codec summary reporting:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Avaya** tab.
4. Click the **IP Network Region DSP/Codec Summary Report** tab. This opens the **IP Network Region DSP/Codec Summary Report** section.
5. Select **Enable Reporting**.
6. Click **Apply Changes**.

Enabling Route Pattern Usage Report

You can use the NNM iSPI for IP Telephony Reporting Configuration form to enable or disable route pattern usage reports.

To configure route pattern usage reporting:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony configuration window opens.
2. Click **Reporting Configuration**. This opens the NNM iSPI for IP Telephony Reporting Configuration form.
3. Click the **Avaya** tab.
4. Click the **Route Pattern Usage Report** tab. This opens the **Route Pattern Usage Report** section.
5. Select **Enable Reporting**.
6. Click **Apply Changes**.

Global IP Telephony Network Management

The 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 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 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 iSPI for IP Telephony Regional Manager Configuration form to add, modify, or delete other NNMi management servers as regional managers.

To access the iSPI for IP Telephony Regional Manager Configuration form:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration...**. The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Regional Manager Configuration**. This opens the iSPI for IP Telephony Regional Manager Configuration form.

The 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.
Description	The description provided while configuring the

Regional Manager Attribute	Description
	regional manager.
UUID	The Universal Unique Identifier (UUID) of the regional manager.
Connection State	<p>The connection state of the regional manager with the global manager. The possible connection states are as follows:</p> <ul style="list-style-type: none">• Not Established• Partial Connection• Connected• Not Connected <p>See the <i>NNMi Online Help</i> for more information about the regional manager connection states.</p>

Adding a Regional Manager Configuration

Before adding a regional network manager to the global network manager, see the *NNMi Online Help* for prerequisites and any additional information required to configure a regional manager with a global manager.

To add a regional manager configuration:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Regional Manager Configuration**. This opens the iSPI for IP Telephony Regional Manager Configuration form.
3. Click **New ***. This opens the Regional Manager Configuration form. This form displays the details in two panels, the left and the right panel.
4. Type the required **Name** and the **Description** for the regional manager in the respective boxes on the left panel.
5. Click **New ***, present under the **Connections** tab on the right panel. This opens the Add IP Telephony Regional Manager Connection form. The **Connections** tab displays the details (marked with an asterisk (*) in the following step) of the connections configured for the regional manager.

Note: You must configure at least one connection for a regional manager.

6. Specify the following details for the connection to the regional manager in the Add IP Telephony Regional Manager Connection form. You can configure multiple connections to a regional manager to support application failover:

- **Hostname***: The official Fully-Qualified-Domain-Name (FQDN) of the Regional Manager.
- **Use Encryption**:
 - If disabled, NNMi uses hypertext transfer protocol (HTTP) and plain sockets to access this Regional NNMi management server.
 - If enabled, NNMi uses secure sockets layer encryption (HTTPS/SSL) to access this Regional NNMi management server.
- **HTTP(S) Port***: The port number for HTTP or HTTPS access to the iSPI for IP Telephony sever on the regional manager The default port numbers are as follows:
 - HTTP: 10080
 - HTTPS: 10443. You must type this value in the **HTTP(S) Port** box if you mark **Use Encryption**.

Note: If you are not using the default values for the ports, check the values 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.
- **User Password**: The password for the user name provided,
- **Ordering***: Provide a numeric value in this box. NNMi checks for configuration settings in the order you define (lowest number first). NNMi uses the first match found for each address. Provide a unique connection ordering number for each Regional Manager configuration.


7. Click **Save**  to add the new regional manager configuration.

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

To modify the configuration details of an existing regional manager:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Regional Manager Configuration**. This opens the iSPI for IP Telephony Regional Manager Configuration form.
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 iSPI for IP Telephony Regional Manager Configuration form.
6. Repeat *step 3* in this procedure.

7. Select the connection that you want to update from the **Connections** tab on the right panel and click **Open** . This opens the Modify IPT Regional Manager Connection form.

Note: The 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 iSPI for IP Telephony process on the active connection, wait for the application failover to complete (the 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.

8. Update the following details in the form as required:

- **Use Encryption:**
 - If disabled, NNMi uses hypertext transfer protocol (HTTP) and plain sockets to access this Regional NNMi management server.
 - If enabled, NNMi uses secure sockets layer encryption (HTTPS/SSL) to access this Regional NNMi management server.
- **HTTP(S) Port:** : The port number for HTTP or HTTPS access to the iSPI for IP Telephony sever on the regional manager The default port numbers are as follows:
 - HTTP: 10080
 - HTTPS: 10443

Note: If you are not using the default values for the ports, check the values 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.
- **User Password:** The password for the user name provided.
- **Ordering:** Provide a numeric value in this box. NNMi checks for configuration settings in the order you define (lowest number first). NNMi uses the first match found for each address. Provide a unique connection ordering number for each Regional Manager configuration.


9. Click **Save**  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. See the *NNMi Online Help* for more information about removing nodes associated to a regional manager.

To delete a regional manager configuration:

1. From the **Workspaces** navigation pane, click **Configuration > iSPI for IP Telephony Configuration...** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Regional Manager Configuration**. This opens the iSPI for IP Telephony Regional Manager Configuration form.
3. Select the regional manager from the *Configured Regional Managers* section and click **Open** . This opens the Regional Manager Configuration form.

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 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 iSPI for IP Telephony process running on the active connection and then delete the connection.

5. Click **Save** and return back to the 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.

Configuring Discovery and Custom Attributes Settings

You can use the NNM iSPI for IP Telephony Discovery Configuration form to configure the discovery settings for the Avaya primary servers. You can also use this form to configure the custom attributes settings for Avaya and Cisco IP Phones.

To access the Discovery Configuration form:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration window opens.
2. Click **Discovery Configuration**. This opens the NNM iSPI for IP Telephony Discovery Configuration form.

Click the following links to know more about configuring discovery and custom attributes settings for IP Telephony devices:

[Configuring Discovery Settings for Avaya Primary Servers](#)

[Configuring Custom Attributes Settings for Avaya IP Phones](#)

[Configuring Custom Attributes Settings for Cisco IP Phones](#)

Configuring Discovery Settings for Avaya Primary Servers

You can use the NNM iSPI for IP Telephony Discovery Configuration form to configure the discovery settings for the Avaya primary servers. You can also use this form to configure the custom attributes settings for Avaya IP Phones.

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. This might impact the call processing.

You can configure the discovery interval for the Avaya primary servers considering the following recommendations. It is recommended to 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:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration....** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **Discovery Configuration**. This opens the NNM iSPI for IP Telephony Discovery Configuration form.
3. Under the **Discovery Configuration** section, clear the **Use NNMi node discovery interval?** 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 (see the next step).

4. Type 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.
5. Select **Pause state pollers during discovery?** check box. If you select this check box, the iSPI for IP Telephony pauses 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 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 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 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

6. Click **Apply Changes**.

Configuring Custom Attributes Settings for Avaya IP Phones

You can use the NNM iSPI for IP Telephony Configuration form to configure the custom attributes settings for the Avaya 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. If 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 custom attributes for Avaya IP Phones:

1. In the NNM iSPI for IP Telephony Discovery Configuration form, select **Avaya** and click the **IP Phones** tab.
2. Under the **Discovery Configuration** section, select the **Enable Phone Custom Attribute Setting?** check box.
3. Click **Apply Changes**.

Note: You must not enable the custom attributes for Avaya IP Phones, if these phones are not discovered in NNMi database.

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:

1. In the NNM iSPI for IP Telephony Discovery Configuration form, select **Cisco** and click the **IP Phones** tab.
2. Under the **Discovery Configuration** section, select the **Enable Phone Custom Attribute Setting?** check box.
3. Click **Apply Changes**.

Note: You must not enable the custom attributes for Cisco IP Phones, if these phones are not discovered in NNMi database.

Managing the Lifecycle of NNMi Nodes Hosting IP Telephony Devices

To manage the lifecycle of NNMi nodes that host the IP Telephony services such as Cisco Voice Gateway, Cisco Unified Communications Manager, Avaya Media Gateway, Avaya Communications Manager and so on, do as follows:

1. Select the IP telephony device that you want to start or stop monitoring from the **Inventory > Node > Node - Nodes** view.
2. Click **Actions > Management Mode** from the menu on the NNMi console. This displays the following options that you can use to start or stop discovery and monitoring of the IP telephony devices:
 - **Manage**—select this option to monitor the status of the selected node.
 - **Manage (Reset All)**—select this option to specify that 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**—select this option to specify that the selected node must not be monitored. After you select this option, the iSPI for IP Telephony stops monitoring the status of the selected node.
 - **Out of Service**—select this option to specify that the selected node is out of service. After you select this option, the 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: <ul style="list-style-type: none">• Marks the status of the call controller as not monitored

IP Telephony Device	Action—Result
	<ul style="list-style-type: none"> • 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 <p>Not Managed:</p> <ul style="list-style-type: none"> • 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	<p>Out of Service:</p> <ul style="list-style-type: none"> • 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 <p>Not Managed:</p> <ul style="list-style-type: none"> • 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
Gatekeeper	<p>Out of Service:</p> <ul style="list-style-type: none"> • 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 <p>Not Managed:</p> <ul style="list-style-type: none"> • 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

IP Telephony Device	Action—Result
Unity Device	<p>Out of Service:</p> <ul style="list-style-type: none"> • 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 <p>Not Managed:</p> <ul style="list-style-type: none"> • Marks the status of the unity device as not monitored. • Changes the management state of the gatekeeper in the node form to unmanaged
IP Phone	<p>Out of Service:</p> <ul style="list-style-type: none"> • 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 <p>Not Managed:</p> <ul style="list-style-type: none"> • 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 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	<p>Out of Service:</p> <ul style="list-style-type: none"> • Marks the status of the primary server as not monitored • Stops polling the primary server for the status

IP Telephony Device	Action—Result
	<ul style="list-style-type: none"> • 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 <p>Not Managed:</p> <ul style="list-style-type: none"> • 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	<p>Out of Service:</p> <ul style="list-style-type: none"> • 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 <p>Not Managed:</p> <ul style="list-style-type: none"> • 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
LSP	<p>Out of Service:</p> <ul style="list-style-type: none"> • 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 <p>Not Managed:</p> <ul style="list-style-type: none"> • Marks the status of the LSP as not monitored. • Stops polling the LSP for the status

IP Telephony Device	Action—Result
	<ul style="list-style-type: none"> Changes the management state of the LSP in the Call Controller form to unmanaged
CLAN, IPSI, or Media Processor	<p>Out of Service:</p> <ul style="list-style-type: none"> 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 <p>Not Managed:</p> <ul style="list-style-type: none"> 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 Phone	<p>Out of Service:</p> <ul style="list-style-type: none"> 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 <p>Not Managed:</p> <ul style="list-style-type: none"> 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 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 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 iSPI for IP Telephony entities from the NNMi node inventory, do as follows:

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 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 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 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 iSPI for IP Telephony to process traps that contain message codes that you require, do as follows:

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 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 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:

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	<code>com.hp.ov.nms.spi.ipt.services</code>
NNM iSPI for IP Telephony services	<code>com.hp.ov.nms.spi.uc.services</code>
NNM iSPI for IP Telephony discovery	<code>com.hp.ov.nms.spi.ipt.disco</code>
NNM iSPI for IP Telephony discovery	<code>com.hp.ov.nms.spi.uc.disco</code>
NNM iSPI for IP Telephony state poller	<code>com.hp.ov.nms.spi.ipt.statepoller</code>
NNM iSPI for IP Telephony state poller services	<code>com.hp.ov.nms.spi.ipt.services.statepoller</code>
NNM iSPI for IP Telephony state poller notification in a Global Network Management environment	<code>com.hp.ov.nms.statepoller.notification.state.geo</code>
CDR/CMR monitoring and reports	<code>com.hp.ov.nms.spi.ipt.cdr.cisco.collection</code>
NNM iSPI for IP Telephony discovery notification	<code>com.hp.ov.nms.spi.ipt.disco.notification</code>
	<code>com.hp.ov.nms.spi.ipt.rtcp</code>
	<code>com.hp.ov.nms.spi.ipt.monitoring.impl.services</code>
	<code>com.hp.ov.nms.spi.ipt.monitoring.services</code>

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 iSPI for IP Telephony with Clarus IPC. This is an optional integration that you can enable after installing the iSPI for IP Telephony.

To integrate the 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 > 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 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 iSPI for IP Telephony.

We appreciate your feedback!

If an email client is configured on this system, click

[Send Email](#)

If no email client is available, copy the following information to a new message in a web mail client and send the message to **docfeedback@hp.com**.

Product name and version: NNM iSPI for IP Telephony, 9.21

Document title: Online Help

Feedback:

