

# HP Network Node Manager i Software Smart Plug-in for IP Telephony

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

Software Version: 9.00

---

[Online Help: Help for Administrators and Operators](#)

Software Release Date: March 2010



## **PDF Version of iSPI for IP Telephony Online Help**

This document is a PDF version of the iSPI for IP Telephony 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 format. You may encounter formatting problems or unreadable text in certain document locations. Those problem topics can be successfully printed from within the online help.

## HP Network Node Manager

### 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 Notices

© Copyright 2008–2010 Hewlett-Packard Development Company, L.P.

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.

#### 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.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

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

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

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 USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065. For the full Oracle license text, see the license-agreements directory on the NNMI product DVD.

## Table of Contents

---

<b>PDF Version of iSPI for IP Telephony Online Help</b> .....	<b>3</b>
<b>HP Network Node Manager</b> .....	<b>4</b>
Legal Notices.....	4
<b>Table of Contents</b> .....	<b>6</b>
<b>HP Network Node Manager i Software Smart Plug-in for IP Telephony</b> .....	<b>12</b>
Getting Started with the iSPI for IP Telephony.....	12
Help for Administrators.....	12
Specify the Range of Extensions for Cisco and Avaya Phones to be Excluded from Discovery . . and Monitoring.....	13
Specifying the Range of Phones to be Excluded.....	14
Configure Data Access.....	15
Configure Data Access for Cisco.....	15
Configure Data Access for Avaya.....	17
Creating Customized CDR Format Specification Files.....	18
Configure Data Access for Nortel.....	19
Configuring Monitoring Tasks.....	20
Configuring Monitoring Tasks Related to Cisco IP Telephony.....	20
Configure the Monitoring for Registration State and Controller Association of IP Phones ..	21
Configure the Monitoring of Call Managers.....	21
Configure the Monitoring of Voice Gateway Channels.....	22
Configure the Monitoring of Voice Gateway Interfaces.....	23
Configure the Monitoring of Gatekeepers.....	24
Configure the Monitoring of Voice Mail Devices.....	24
Configuration for Survivable Remote Site Telephony (SRST) and Call Manager Express ... (CME) monitoring.....	25
Configuring Monitoring Tasks Related to Avaya IP Telephony.....	25
Configure the Monitoring for CLAN and IP Phone Association.....	26
Configure the Monitoring for IP Phones.....	26
Configure the Monitoring for Media Processors.....	27
Configure the Monitoring for IP Server Interfaces.....	27
Configure the Monitoring for IP Network Regions.....	28
Configure the State Monitoring for the Duplex Primary Servers.....	28
Configure the State Monitoring for Survivable Servers.....	29

---

Configure the Monitoring for Media Gateways.....	29
Configure the Monitoring for Route Pattern Usage Metrics.....	31
Configure the Monitoring for Trunk Groups.....	31
Configure the Monitoring of Processor Occupancy for Communication Managers.....	32
Configure the Monitoring of Port Network Load Statistics.....	32
Configuring Monitoring Tasks for Nortel IP Telephony.....	32
Configuring QoS Zones Monitoring.....	33
Configure the Monitoring of IP Phones.....	33
Configure the QOS and MOS Monitoring Threshold Values for Cisco.....	34
Reporting Configuration.....	34
Configure Cisco CDR Reporting.....	34
Configure Avaya CDR Reporting.....	35
Managing the Lifecycle of NNMi Nodes Hosting IP Telephony Devices.....	35
Managing Cisco IP Telephony Devices.....	36
Managing Avaya IP Telephony Devices.....	38
Deleting IP Telephony Entities from the iSPI for IP Telephony.....	40
Logging and Tracing.....	41
To set the trace level:.....	41
Integration with ClarusIPC.....	42
Help for Operators.....	42
IP Telephony Inventory.....	43
Monitoring Cisco Call Controllers.....	44
To launch the Call Controllers view:.....	44
Cisco Call Controller Details Form.....	45
Monitoring Cisco IP Phones.....	47
To launch the IP Phones view:.....	47
Filtering Cisco IP phones.....	47
To filter the IP Phones view:.....	48
Cisco Extension Details form.....	48
Monitoring Cisco IC Trunks.....	49
To launch the Cisco IC Trunks view.....	49
H323 Trunk Details Form.....	50
Monitoring Cisco Gatekeepers.....	50
To launch the Cisco Gatekeepers view.....	51
Cisco GateKeeper Details Form.....	51

---

---

Monitoring Voice Gateways .....	52
To launch the Cisco Voice Gateways view.....	52
Viewing Cisco Voice Gateway Endpoints.....	52
To launch the Node form for a Cisco Voice Gateways device.....	53
Node Form: Voice Gateway Interfaces Tab.....	53
Viewing Cisco Voice Gateway Endpoint Channels.....	54
To launch the Node form to view endpoint channel details of a Cisco Voice Gateway .... device.....	54
Node Form: Voice Gateway Channels Tab.....	54
Monitoring Cisco Unity Devices.....	55
To launch the Cisco Unity Devices view.....	55
Cisco Unity Devices Form.....	56
ClarusIPC Integration–Test Plans and Test Result Reports.....	56
Monitoring Nortel Call Servers.....	56
To launch the Call Servers view.....	56
Nortel Call Server form.....	57
Monitor Nortel Signaling Servers.....	58
To launch the Nortel Signaling Servers view.....	58
Nortel Signaling Server Details Form.....	59
Nortel IP Phones View.....	59
To launch the IP Phones view.....	60
View the Nortel Phone Detailed form.....	60
Nortel Phone Detailed form.....	60
Monitoring Nortel media gateways.....	61
To launch the Nortel Media Gateways view.....	61
.....	61
View the Nortel Media Gateway form.....	61
View the Nortel Media Gateway Details Form.....	62
Nortel QOS Zones Table View.....	62
To launch the Nortel QOS Zones table view.....	62
.....	63
View the Nortel QOS Zone Details form.....	63
View the Nortel QOS Zone Details Form.....	63
Monitoring Avaya Call Controllers.....	65
To launch the Avaya Call Controllers view:.....	65

---



---

Avaya Call Controller Details Form.....	65
Monitoring Network Regions.....	67
IP Network Region Detail Form.....	67
Monitoring IP Media Processor DSP Resource Metrics.....	69
Specifying Threshold Values for Metrics.....	70
IP Network Region Connection Detail Form.....	70
Monitoring Route Patterns.....	71
Route Pattern Detailed Form.....	71
Monitoring Trunk Group Usage.....	72
Monitoring Trunk Groups.....	73
Trunk Group Detailed Form.....	73
Monitoring Trunk Group Members.....	74
Trunk Group Member Detailed Form.....	75
Monitoring Signaling Groups.....	76
Signaling Group Details Form.....	76
Monitoring Processor Occupancy Metrics.....	77
Specifying Threshold Values for Metrics.....	77
Monitoring Avaya IP Phones.....	78
To launch the Avaya IP Phones view:.....	78
Filtering Avaya IP phones.....	78
To filter the Avaya IP Phones view:.....	79
Avaya IP Phones Details Form.....	79
	80
Monitoring Avaya Port Networks.....	80
To launch the Port Networks view:.....	80
Port Network Detail Form.....	81
The left pane lists the general attributes of the port network as shown in the following table..	81
Monitoring IP Server Interface.....	82
IP Server Interface Details Form.....	82
	83
Status of the IPSI.....	83
Monitoring CLAN.....	83
CLAN Details Form.....	83
Monitoring Media Processors.....	85

---

---

Media Processor Details Form.....	85
Status Attributes.....	87
Monitoring Port Network Load Details Metrics.....	87
Specifying Threshold Values for Metrics.....	88
Monitoring Total Load Metrics.....	88
Specifying Threshold Values for Metrics.....	88
Monitoring Intercom Load Metrics.....	89
Specifying Threshold Values for Metrics.....	89
Monitoring Incoming Trunk Load Metrics.....	89
Specifying Threshold Values for Metrics.....	90
Monitoring Outgoing Trunk Load Metrics.....	90
Specifying Threshold Values for Metrics.....	90
Monitoring Tandem Trunk Load Metrics.....	91
Specifying Threshold Values for Metrics.....	91
Monitoring Media Gateways.....	91
To launch the Media Gateways view:.....	91
Media Gateway Details Form.....	92
Monitoring Media Modules.....	94
Media Modules Form.....	94
Monitoring VOIP Engines.....	95
VOIP Engines Form.....	95
Monitoring DSP Cores.....	96
DSP Cores Form.....	97
Incidents Collected from the ClarusIPC Environment.....	97
Context-Sensitive URLs for ClarusIPC Incidents.....	98
Incidents generated by the iSPI for IP Telephony.....	99
Viewing the Network Connectivity.....	117
Launch a Voice Path.....	118
Launch a Control Path.....	118
Launch the HTTP to Phone Path.....	119
Integration with the iSPI Performance for Quality Assurance.....	119
Reference Information.....	120
Name.....	120
Synopsis.....	120

---

---

DESCRIPTION.....	120
EXAMPLES.....	120
AUTHOR.....	120
FILES.....	121
Name.....	121
Synopsis.....	121
DESCRIPTION.....	121
PARAMETERS.....	121
	122
EXAMPLES.....	122
AUTHOR.....	122
FILES.....	122
<b>Index</b> .....	<b>123</b>

## HP Network Node Manager i Software Smart Plug-in for IP Telephony

The HP Network Node Manager i Software Smart Plug-in for IP Telephony (**iSPI for IP Telephony**) extends the capability of NNMi to monitor and manage the IP telephony infrastructure in your network environment. The iSPI for IP Telephony presents additional views, incidents, reports, and so on for you to manage the IP telephony deployment in your enterprise.

The iSPI for IP Telephony, in conjunction with NNMi, helps you perform the following tasks:

- Discover IP Telephony entities representing IP telephony devices, functions, services and resources and the corresponding configuration properties required for subsequent monitoring and diagnostics.
- Monitor changes of various types of states for IP telephony entities
- Monitor the usage and performance related metrics for the IP telephony functions and resources
- Monitor the Call Quality metrics (MOS, Jitter, Latency, Packet-loss) for calls
- Run reports on Call Quality metrics for the calls in the enterprise
- Run reports on Call Volume, Call Duration for various Call Traffic analysis
- Perform L2/L3 diagnostics for IP Telephony issues by navigating to L2/L3 views from NNMi or by launching Control/Voice Path for IP Phones
- Run IP Telephony end user service tests such as testing ability to handle requests for configured call features for endpoints or testing whether configurations are honored for endpoints
- Track changes in configuration between time intervals
- View test result reports for network layer quality of service tests configured on routers in the voice path between arbitrary pair of IP Phones.

After you install (and configure) the iSPI for IP Telephony on the NNMi management server, the same instance of iSPI for IP Telephony allows you to perform the various management tasks for IP telephony deployments from different vendors such as Cisco, Avaya or Nortel.

### Getting Started with the iSPI for IP Telephony

See the *HP NNM i Software Smart Plug-in for IP Telephony Installation Guide* for more information on the following topics:

- Configuration tasks on NNMi before installing the iSPI for IP Telephony
- Installation of the iSPI for IP Telephony
- Initial configuration tasks on NNMi and iSPI for IP Telephony

After you complete the tasks listed, you can start using the iSPI for IP Telephony. See the *HP NNM i Software Smart Plug-in for IP Telephony Installation Guide* for more information.

### Help for Administrators

As an administrator, you can configure the 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 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

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.

As an administrator you can also enable or disable integration of the 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 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:

- [Configuring Monitoring Tasks](#)
- [Managing the Lifecycle of NNMi Nodes Hosting IP Telephony Devices](#)
- [Deleting IP Telephony Entities from the iSPI for IP Telephony](#)
- [Logging and Tracing](#)
- [Integration with ClarusIPC](#)

## Specify the Range of Extensions for Cisco and Avaya Phones to be Excluded from Discovery and Monitoring

You can specify the range of extensions for phones to be excluded from being discovered and monitored for both Avaya and Cisco. After you specify the phones and apply the changes, the iSPI for IP Telephony removes the specified phones from the IP Phones table and does not manage or monitor these phones. The iSPI for IP Telephony does not discover these phones in the subsequent discovery cycle.

#### To specify the range of extensions for Cisco phones to be excluded from discovery and monitoring:

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 **Cisco** tab.
4. In **Value** box for the **Cluster ID** section, specify the ID of the cluster 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 ["Specify the Range of Extensions for Cisco and Avaya Phones to be Excluded from Discovery and Monitoring" \(on page 13\)](#) for more information about specifying extension ranges to be excluded from discovery and monitoring.
6. Click **Apply Changes**.

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

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. Type the ID of the cluster for which you had specified the exclusion filter in the **Cluster ID** box in the Delete IP Phone Exclusion filter section
4. Click **Delete**.

**To specify the range of extensions for Avaya phones to be excluded from discovery and monitoring:**

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 **Value** box for 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.
5. In the **Filter** section, specify the extension range to be excluded in the **Value** box. See the section ["Specify the Range of Extensions for Cisco and Avaya Phones to be Excluded from Discovery and Monitoring" \(on page 13\)](#) for more information about specifying extension ranges to be excluded from discovery and monitoring.
6. Click **Apply Changes**.

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

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. Type the IP address of the communication manager for which you had specified the exclusion filter in the **CM IP Address** box in the Delete IP Phone Exclusion filter for a cluster section
4. Click **Delete**.

## 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.

## Configure Data Access

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

## Configure 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

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

### To configure AXL access for Cisco:

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 **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:
  - **Cluster ID:** specifies the cluster identifier. You can retrieve this information from the administration web page of the Cisco Unified Communications Manager.
  - **CM IP Address:** specifies the IP address of the Cisco Unified Communications Manager (CM) server node in this cluster. The iSPI for IP Telephony uses this IP address to obtain the AXL data for this cluster. It is recommended that you provide the IP address of the publisher CM node in your 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**.

### To delete an AXL access configuration for a cluster:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Cisco** tab and then click the **AXL Access** tab.
2. Specify the cluster ID of the cluster that you want to delete in the **Cluster ID** box in the **Delete AXL access configuration for a cluster** section.
3. Click **Delete** to delete the AXL access configuration on the specified cluster.

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

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

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 **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 in the **Value** box for each of the following parameters:
  - **Cluster ID:** specifies the cluster identifier. You can retrieve this information from the administration web page of the Cisco Unified Communications Manager.
  - **Server IP:** specifies the IP address of the Cisco Call Manager CDR repository server in the cluster where the CDRonDemand Web Service is running..
  - **SOAP User Name:** specifies the SOAP user name to access the CDRonDemand Web Service in the cluster.
  - **SOAP Password:** specifies the password for the user name specified.
  - **Port:** specifies the port number used by the CDRonDemand Web Service on the server that hosts the Web Service.
6. Click **Add/Modify**.

**To configure FTP credentials to be used by CDRonDemand Web Service to send the CDR files to the 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.

**Note:** If the iSPI for IP Telephony is installed on a Microsoft Windows operating system, you must make sure that the home directory for the user specified in *FTP user name* is configured as %NnmD-ataDir%\log\ipt\tmp and the user has *write* access to the home directory. This step is required only if you are running the iSPI for IP Telephony on Microsoft Windows operating systems.

4. Click **Apply**



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

**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. Specify the cluster ID of the cluster for which you want to delete the CDR access configuration in the iSPI for IP Telephony in the **Cluster ID** box.
3. Click **Delete**

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

The **Current Configurations for accessing CDR on Demand Web Service in Cisco Unified Communications Manager Cluster** section lists the configured clusters from which the iSPI for IP Telephony accesses the CDR data.

### Configure 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 using SFTP.
  - **SFTP User Name:** specifies the Secure File Transfer Protocol (SFTP) user name to be used by the iSPI for IP Telephony to access or download the CDR files from the communication manager server.
  - **SFTP Password:** specifies the SFTP password for the user name specified.
  - **CDR Format:** specifies the CDR format configured on the communication manager server.
  - **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

- **Data 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.
- **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 iSPI for IP Telephony server. You must prepare this file for each communication manager server before configuring the 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](#).
- **Time Zone:** specifies the time zone of the communication manager server in GMT+/- HH:MM format. Note that you must specify the time zone only in this format. For example, if you want to specify the Pacific Time (US & Canada), specify the time as GMT-08:00.

6. Click **Add/Modify**

**Note:** You must configure the iSPI for IP Telephony to collect CDR data from all the communication manager servers in your deployment environment including the standby duplex servers (for example, the standby s87xx servers) and the survivable .servers (for example, the s83xx LSP servers) by adding the physical IP addresses for each of these servers, the associated credentials for CDR SFTP access, and the associated CDR format information.

The **Current Configurations** section lists the number of 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. Specify the IP address of the communication manager in the **Communication Manager IP Address** box.
3. Click **Delete** to delete the specified Avaya IPT CDR access configuration.

## 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.
```

## iSPI for IP Telephony 9.00 Online Help

### HP Network Node Manager i Software Smart Plug-in for IP Telephony

```
# 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=
```

### Configure 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 **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:** specifies the Embedded LAN (ELAN) IP address of the signaling server.
  - **TLAN IP Address:** specifies the Telephony LAN (TLAN) IP address of the signaling server.

- **Auto accept Host Key?:** specifies if the host key must be accepted automatically for the signaling server. Select **True** to enable this feature.
- **Host Key Algorithm?:** specifies the host key algorithm. You can select one of the following algorithms:
  - **ssh-rsa:** specifies authentication using the ssh-rsa key pair.
  - **ssh-dss:** specifies authentication using the ssh-dss key pair.
- **Host Key HexFingerprint:** specifies the host key fingerprint in hexadecimal format.
- **User Name:** specifies the user name to log on to the signaling server.
- **Password:** specifies 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**.

#### To delete an SSH access configuration:

1. On the NNM iSPI for IP Telephony Data Access Configuration page, click the **Nortel** tab.
2. Specify the ELAN IP address of the signaling server that you want to delete in the **ELAN IP Address of Signaling Server** box.
3. Click **Delete** to delete the .

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

## 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" \(on page 20\)](#)
- ["Configuring Monitoring Tasks Related to Avaya IP Telephony" \(on page 25\)](#)
- ["Configuring QoS Zones Monitoring" \(on page 33\)](#)

## Configuring Monitoring Tasks Related to Cisco IP Telephony

Click the **Cisco** tab to specify the following Monitoring Configurations:

- [Configuration for monitoring Registration State & Controller Association of IP Phones](#)
- [Configuration for Call Manager State monitoring](#)
- [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 \(SRST\) and Call Manager Express \(CME\) monitoring](#)

### Configure the Monitoring for Registration State and Controller Association of IP Phones

After the 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 **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 **Configuration for Monitoring Registration State and Controller Association of IP Phones** section, specify the following details:
  - **Monitor** Select **True** 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 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**.

### Configure the Monitoring of Call Managers

After the 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 **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 Call Manager State Monitoring** section, specify the following details:
  - **Monitor:** Set this option to **True** 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 iSPI for IP Telephony waits for before declaring that a channel is Idle:

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 **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:** Set this option to **True** 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 600 seconds. For example if you specify 600 seconds as the waiting time and period of the usage state monitoring for channels is 120 seconds, then, during the monitoring of usage state for channels, if the iSPI for IP Telephony finds the usage state to be Idle, the iSPI for IP Telephony waits for 5 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 **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:
  - **Monitor:** Set this option to **True** 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**.

**To configure the monitoring for the operational state of voice gateway channels:**

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 **Voice Gateway Channel** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for Voice Gateway Channel Operational State monitoring** section, specify the following details:
  - **Monitor:** Set this option to **True** to monitor the operational states of voice gateway channels.
  - **Interval:** Specify the interval (in seconds) to poll the operational states of 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 **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:
  - **Monitor:** Set this option to **True** 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 **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:

- **Monitor** Set this option to **True** 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 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 **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 Gatekeepers' count of registered endpoints** section, specify the following details:
  - **Monitor:** Set this option to **True** if you want 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 **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:
  - **Monitor:** Set this option to **True** 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 Voice Mail Devices

In the **Voice Mail Devices** tab on the Cisco Call Controller detail view, the 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 Voice Mail Devices monitoring:**

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 **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:
  - **Monitor:** Set this option to **True** if you want 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) and Call Manager Express (CME) monitoring**

After the iSPI for IP Telephony discovers the available Cisco SRST routers and the Cisco Call Manager Express services 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) and Call Manager Express (CME) State Monitoring:**

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 **SRSTs and CMEs** tab on the NNM iSPI for IP Telephony Monitoring Configuration form.
4. In the **Configuration for Survivable Remote Site Telephony (SRST) and Call Manager Express (CME) State Monitoring** section, specify the following details:
  - **Monitor:** Set this option to **True** to monitor the states of SRST and Call Manager Express routers.
  - **Interval:** Specify the frequency (in seconds) to monitor the states the routers. The default value is 300 seconds.
5. Click **Apply Changes**.

**Configuring Monitoring Tasks Related to Avaya IP Telephony**

Click the **Avaya** tab to specify the following monitoring configuration changes:

- [Configure the Monitoring for CLAN and IP Phone Association](#)
- [Configure the Monitoring for IP Phones](#)
- [Configure the Monitoring for Media Processors](#)

- [Configure the Monitoring for IP Server Interfaces](#)
- [Configure the Monitoring for IP Network Regions](#)
- [Configure the State Monitoring for the Duplex Primary Servers](#)
- [Configure the State Monitoring for Survivable Servers](#)
- [Configure the Monitoring for Media Gateways](#)
- [Configure the Monitoring for Route Pattern Usage Metrics](#)
- [Configure the Monitoring for Trunk Groups](#)
- [Configuring Polling for Port Network Load Statistics](#)
- [Configure the Monitoring of Processor Occupancy for Communication Managers](#)
- [Configure the Monitoring of Port Network Load Statistics](#)

### Configure the Monitoring for CLAN and IP Phone Association

The 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.

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

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 **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:
  - **Monitor:** Set this option to **True** 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 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 **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:
  - **Monitor:** Set this option to **True** 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**.

### **Configure the Monitoring for Media Processors**

The 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 **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:
  - **Monitor:** Select **True** 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 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 **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:

- **Monitor:** Select **True** to enable the monitoring for 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 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 **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:
  - **Monitor:** Select **True** to enable the monitoring for IP Network Regions.
  - **Interval:** Specify the monitoring interval (in seconds). The default interval is 300 seconds.
6. Click **Apply Changes**.

**Note:** As part of Avaya IP Network Region Monitoring, the iSPI for IP Telephony generates incidents for any breach of threshold values in any of the parameters related to the usage and performance of DSPs and CODECs deployed in various Network Regions. You can set the threshold values for each of these IP Network Region DSP and CODEC summary metrics by using the Avaya Network Region detail form. See the section [Monitoring IP Media Processor DSP Resource Metrics](#) for more information.

### Configure the State Monitoring for the Duplex Primary Servers

The 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 **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:
  - **Monitor:** Select **True** 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 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 **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:
  - **Monitor:** Select **True** 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 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 **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:
  - **Monitor:** Set this option to **True** 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:
  - **Monitor:** Set this option to **True** 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 VoIP Engine States:**

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 Engine States** section, specify the following details:
  - **Monitor:** Set this option to **True** to monitor the media gateway VoIP Engine states.
  - **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 DSP Core States:**

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:
  - **Monitor:** Set this option to **True** 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 **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:
  - **Monitor:** Select **True** 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**.

**Note:** As part of Avaya Route Pattern Usage Monitoring, the iSPI for IP Telephony generates incidents for any breach of threshold value for the parameter named `Queue Overflow Threshold` for a Route Pattern. You can set the threshold value for this parameter by using the Route Pattern detail form. See the section [Route Pattern Detailed Form](#) for more information.

### 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 **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:

- **Monitor:** Select **True** 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:
  - **Monitor:** Select **True** 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 of Processor Occupancy for Communication Managers

The iSPI for IP Telephony continuously monitors the hourly Processor Occupancy summaries for each Communication Manager (CM) that is discovered by the iSPI for IP Telephony and generates incidents on breach of threshold values for any of the Processor Occupancy related summary metrics. In order to set the thresholds for these metrics for a specific CM, open the Communication Manager detail form and then go to the Processor Occupancy detail form. See the section [Monitoring Processor Occupancy Metrics](#) for more information.

#### Configure the Monitoring of Port Network Load Statistics

The iSPI for IP Telephony continuously monitors the hourly Port Network Load Statistics for various types of loads on each Port Network object that is discovered by the iSPI for IP Telephony and generates incidents on breach of threshold values for any of the Port Network Load related summary metrics. You can set the thresholds for these metrics for a specific Port Network by launching the detail form for the Port Network. See the section [Port Network Detail Form](#) for more information.

#### Configuring Monitoring Tasks for Nortel IP Telephony

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

- [Configuring QoS Zones Monitoring](#)
- [Configure the Monitoring of IP Phones](#)



## Configuring QoS Zones Monitoring

The iSPI for IP Telephony monitors the various QoS-related measurements in the Nortel QoS Zones. The 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 **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:
  - **Monitor:** Set this option to **True** 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**.

**Note:** As part of Nortel QOS Zone Monitoring, the iSPI for IP Telephony generates incidents for any breach of threshold values for any of the monitored parameters for Nortel QOS zones. You can set the thresholds for each of the Nortel QOS Zone parameters by using the Nortel QOS Zone detail form. See the section [Set thresholds for Nortel QoS metrics](#) for more information.

## 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 **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:
  - **Monitor:** Set this option to **True** 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**.

## Configure the QOS and MOS Monitoring Threshold Values for Cisco

The Cisco IP Telephony QOS/MOS Monitor Thresholds Configuration form allows you to specify the threshold values for the 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 iSPI for IP Telephony generates an incident conveying the resulting values and the set threshold.

### To configure the QOS and MOS Monitoring Threshold values:

1. From the **Workspaces** navigation pane, click **iSPI for IP Telephony Configuration...** The NNM iSPI for IP Telephony Configuration form opens.
2. Click **QOS/MOS Monitor Threshold Configuration**. This opens the Cisco IPT QOS/MOS Monitor Thresholds Configuration form.
3. Specify the following QOS and MOS monitoring threshold values as required in the **Value** box adjacent to the threshold.

QOS/MOS Monitoring Threshold	Description
Jitter	Specifies the jitter threshold to be configured in milliseconds. The default value is -1.
PPL	Specifies the Percentage Packet Loss (PPL) threshold to be configured. The default value is 50%. To specify a percentage packet loss threshold of 50%, type 50 here.
Latency	Specifies the latency threshold to be configured in milliseconds. The default value is -1.
MOS	Specify the value in hundreds. For example to specify MOS threshold of 3.6, type 36.
RTT	Specifies the Round Trip Time (RTT) in milliseconds. The default value is -1.

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

## 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 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 **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 CDR 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 **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. Select **True** for **Enable Cisco CDR Reporting?** to enable Cisco CDR reporting.
5. Click **Apply Changes**.

#### Configure Avaya CDR 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 **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. Select **True** for **Enable Avaya CDR Reporting?** to enable Avaya CDR reporting.
5. Click **Apply Changes**.

### 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	<p>Out of Service:</p> <ul style="list-style-type: none"> <li>• Marks the status of the call controller as not monitored</li> <li>• Stops polling the call controller for the status</li> <li>• Changes the registration state of the phones associated with the call controller as unknown</li> <li>• Changes the management state of the call controller in the Call Controller form to Out of Service</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the call controller as not monitored</li> <li>• Stops polling the call controller for the status</li> <li>• Changes the registration state of the phones associated with the call controller as unknown</li> <li>• Changes the management state of the call controller in the Call Controller form to unmanaged.</li> </ul>
Voice Gateway	<p>Out of Service:</p> <ul style="list-style-type: none"> <li>• Marks the status of the voice gateway as not monitored.</li> <li>• Stops polling the voice gateway for the status</li> </ul>

IP Telephony Device	Action—Result
	<ul style="list-style-type: none"> <li>• Changes the management state of the voice gateway in the node form to out of service</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the voice gateway as not monitored.</li> <li>• Stops polling the voice gateway for the status</li> <li>• Changes the management state of the voice gateway in the node form to unmanaged</li> </ul>
Gatekeeper	<p>Out of Service:</p> <ul style="list-style-type: none"> <li>• Marks the status of the gatekeeper as not monitored.</li> <li>• Stops polling the gatekeeper for the status</li> <li>• Changes the number of registered endpoints for the gatekeeper to not monitored.</li> <li>• Changes the management state of the gatekeeper in the node form to out of service</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the gatekeeper as not monitored.</li> <li>• Stops polling the gatekeeper for the status</li> <li>• Changes the management state of the gatekeeper in the node form to unmanaged</li> </ul>
Unity Device	<p>Out of Service:</p> <ul style="list-style-type: none"> <li>• Marks the status of the unity device as not monitored.</li> <li>• Changes the management state of the gatekeeper in the node form to out of service</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the unity device as not monitored.</li> <li>• Changes the management state of the gatekeeper in the node form to unmanaged</li> </ul>

IP Telephony Device	Action—Result
IP Phone	<p>Out of Service:</p> <ul style="list-style-type: none"> <li>• Marks the status of the phone as not monitored.</li> <li>• Stops polling the phone for the status</li> <li>• Changes the management state of the phone in the extension details form to out of service</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the phone as not monitored.</li> <li>• Stops polling the phone for the status.</li> <li>• Changes the management state of the phone in the extension details form to unmanaged</li> </ul>

**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"> <li>• Marks the status of the primary server as not monitored</li> <li>• Stops polling the primary server for the status</li> <li>• Changes the registration state of the phones associated with the call controller as unknown</li> <li>• Changes the management state of the call controller in the Call Controller form to Out of Service</li> <li>• Stops the discovery of associated primary server entities such as the network region, the route pattern, the trunk group, and so on</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the primary server as not monitored</li> <li>• Stops polling the primary server for the status</li> <li>• Changes the registration state of the phones associated with the call controller as unknown</li> <li>• Changes the management state of the call controller in the Call Controller form to unmanaged</li> <li>• Stops the discovery of associated primary server entities such as the network</li> </ul>

IP Telephony Device	Action—Result
	region, the route pattern, the trunk group, and so on
Media Gateway	<p>Out of Service:</p> <ul style="list-style-type: none"> <li>• Marks the status of the media gateway as not monitored.</li> <li>• Stops polling the media gateway for the status</li> <li>• Changes the management state of the voice gateway in the Media Gateway Detailed form to out of service</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the media gateway as not monitored.</li> <li>• Stops polling the media gateway for the status</li> <li>• Changes the management state of the media gateway in the Media Gateway Detailed form to unmanaged</li> </ul>
LSP	<p>Out of Service:</p> <ul style="list-style-type: none"> <li>• Marks the status of the LSP as not monitored.</li> <li>• Stops polling the LSP for the status</li> <li>• Changes the management state of the LSP in the Call Controller form to out of service</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the LSP as not monitored.</li> <li>• Stops polling the LSP for the status</li> <li>• Changes the management state of the LSP in the Call Controller form to unmanaged</li> </ul>

IP Telephony Device	Action—Result
CLAN, IPSI, or Media Processor	<p>Out of Service:</p> <ul style="list-style-type: none"> <li>• Marks the status of the device as not monitored.</li> <li>• Stops polling the device for the status</li> <li>• Changes the management state of the device in the corresponding detail form to out of service</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the device as not monitored.</li> <li>• Stops polling the device for the status</li> <li>• Changes the management state of the device in the corresponding detail form to unmanaged</li> </ul>
IP Phone	<p>Out of Service:</p> <ul style="list-style-type: none"> <li>• Marks the status of the phone as not monitored.</li> <li>• Stops polling the phone for the status</li> <li>• Changes the management state of the phone in the phone details form to out of service</li> </ul> <p>Not Managed:</p> <ul style="list-style-type: none"> <li>• Marks the status of the phone as not monitored.</li> <li>• Stops polling the phone for the status.</li> <li>• Changes the management state of the phone in the phone details form to unmanaged</li> </ul>

**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 iSPI for IP Telephony removes the corresponding iSPI for IP Telephony Call Controller entity along with all the references in the 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 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.

## Logging and Tracing

To perform the monitoring task, the iSPI for IP Telephony uses different processes. The iSPI for IP Telephony provides you with log files that capture the states of these processes.

These log files are stored into the following directory:

*On the UNIX management server:* `/var/opt/OV/log/ipt`

*On the Windows management server:* `%NnmDataDir%\log\ipt`

You can set the level of details that can be captured in these log files by setting the trace level appropriately.

### To set the trace level:

1. Open the logging.properties file with a text editor from the following location on the management server:
  - On UNIX: `/var/opt/OV/shared/ipt/conf`
  - On Windows: `%NnmDataDir%\shared\ipt\conf`
2. Set the following properties to **INFO**, **FINE**, or **FINEST** (by default, all properties are set to INFO):
  - level
  - java.util.logging.FileHandler.level
  - com.hp.ov.nms.spi.ipt.statepoller.level
  - com.hp.ov.nms.spi.ipt.services.level
  - com.hp.ov.nms.spi.ipt.content.level
  - com.hp.ov.nms.spi.ipt.level
  - com.hp.ov.nms.apa.level
  - com.hp.ov.nms.analysis.level
  - com.hp.ov.nms.statepoller.level
  - com.hp.ov.nms.disco.level

The FINEST option gives you the most comprehensive level of details.

## 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.

## 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 Call Controllers	View the discovered Cisco Unified Communication Manager (CallManager) servers available on the network.

View	Purpose
Cisco IP Phones	View the discovered Cisco IP phones available on the network.
Cisco IC Trunks	View the discovered Cisco inter-cluster trunks available on the network.
Cisco Gate-keepers	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 Port Networks	View the discovered Avaya port networks available on the network.
Avaya Media Gateways	View the discovered Avaya media gateways available on the network.
Nortel Call Servers	View the discovered Nortel Call Servers available on the network.
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.
Nortel QOS Zones	View the QoS zones configured with the Nortel Signaling Server.

In this document, the Cisco Unified Communication Manager server is referred to as the Cisco Call-Manager 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 Call Controllers

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

### To launch the Call Controllers view:


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


### Basic Attributes of the Cisco Call Controllers Table

Attribute	Description
Status	<p>The Status of the Cisco Call Controller server. Possible values are:</p> <ul style="list-style-type: none"><li>• Normal—indicates the server is UP.</li><li>• Critical—indicates the server is DOWN.</li><li>• No Status—this is indicated before the first polling cycle takes place.</li><li>• Unknown—indicates no SNMP, which indicates the state of the server, is available from the node.</li></ul> <p>The status for an SRST Router can be one of the following:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li><li>• Critical—indicates that the SRST router is down.</li></ul>
Name	The hostname of the Cisco Call Controller server.
IP Address	The IP address of the Cisco Call Controller server.
Version	The version of the Call Controller server.
Type	The type of the Cisco Call Controller Server, for example, Cisco Call Manager, SRST Router, or Cisco Call Manager Express.
Cluster	The name of the cluster to which the Cisco Call Controller server belongs.

You can view the details of a single Call Controller server 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 . The Cisco 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.

## 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, the voice mail devices, and the IP phones configured with an SRST router. The form presents two different panes.

The right pane lists the following details:

- **Associated gatekeepers:** The Associated 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](#).
- **Current Controlled Extensions:** The Associated Extensions 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](#).
- **SRST Configured Extensions:** The SRST Configured Extensions 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 Extensions page](#).
- **Voice Mail Devices:** The Voice Mail Devices tab displays the list of voice mail devices configured with the selected Cisco Call Controller as shown in the [Voice Mail Devices page](#).
- **Incidents:** The incidents generated for the Call Controller state changes.

The left pane lists the following details of the selected Cisco Call Controller.

### Basic Attributes of the Selected Cisco Call Controller

Attribute	Description
Hosted Node	The node on which the Call Controller is hosted.
Name	The name of the Call Controller server.
IP Address	The IP address of the Call Controller server.
Management Mode	The management status of the node. The status can be any of the following strings: <ul style="list-style-type: none"> <li>• <b>Managed:</b> indicates that the node is managed by the iSPI for IP Telephony.</li> <li>• <b>Out of Service:</b> indicates that the node is currently out of service and not managed by the iSPI for IP Telephony.</li> <li>• <b>Unmanaged:</b> indicates that the node is currently not managed by the iSPI for IP Telephony.</li> </ul>
Type	The type of the Cisco Call Controller. The type can be one of the following: <ul style="list-style-type: none"> <li>• Cisco Call Manager</li> <li>• Cisco Call Manager Express</li> <li>• SRST Router</li> </ul>
Version	The version of the server.
Description	A short description of the server.
Cluster	The name of the cluster to which the Cisco CallManager server belongs.

### Call Manager Specific Attributes

Attribute	Description
Cluster	Specifies the version of the Call Manager cluster.

### 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.

### 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.

## Monitoring Cisco 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.


### 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"><li>Registered</li><li>Unregistered</li><li>Unknown</li><li>Rejected</li><li>Partially Registered</li></ul>
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 phone is registered.
SRST Router	The name of the Survivable Remote Site Telephony (SRST) router configured for 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 Cisco IP Phones view, select the node of your interest, and then click . 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.

## 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, and Controller columns.

#### To filter the IP Phones view:

1. Right-click the **Registration State**, **Extension Number**, **IP Address**, **Controller**, or **SRST** attribute of one of the IP phones listed in the IP Phones view.
2. Select one of the following filters:
  - **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.
  - **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.

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	The management status of the node. The status can be any of the following strings: <ul style="list-style-type: none"><li>• <b>Managed</b>: indicates that the node is managed by the iSPI for IP Telephony.</li><li>• <b>Out of Service</b>: indicates that the node is currently out of service and not man-</li></ul>



Attribute	Description
	aged by the iSPI for IP Telephony. <ul style="list-style-type: none"> <li>Unmanaged: indicates that the node is currently not managed by the iSPI for IP Telephony.</li> </ul>
Protocol	The protocol used by the phone.
SRST Router	The name of the SRST router.

## Monitoring Cisco IC Trunks

The IC Trunks view displays a list of available Cisco intercluster trunks in the network. The view arranges the key attributes of all the intercluster trunks in a table.

### To launch the Cisco IC Trunks view

From the **Workspaces** navigation pane, click **Cisco IP Telephony > IC Trunks**. The Cisco IC Trunks view opens in 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"> <li>Registered</li> <li>Unregistered</li> <li>Rejected</li> <li>Unknown</li> <li>Not Applicable (for non-gatekeeper-controlled intercluster trunks)</li> </ul>
Name	The name of the Cisco intercluster trunk.
Type	Type of the intercluster trunk. This field indicates if the intercluster trunk is gatekeeper-controlled 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).
Cluster	The name of the cluster to which the intercluster trunk belongs.
Hosted On	The name of the Cisco CallManager server that hosts the intercluster trunk.

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.

You can view the details of a single Cisco intercluster trunk within a form.

### To view the H323 Trunk form:

In the Cisco IC Trunks view, select the node of your interest, and then click . 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.

### H323 Trunk Details Form

The H323 Trunk form helps you view the node details of the selected Cisco 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 Cisco 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.
Cluster	The name of the cluster to which the intercluster trunk belongs.
Gatekeeper	The IP address of the gatekeeper device that controls the intercluster trunk.

#### 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.

### 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.
H323Endpoints	The number of endpoints associated with 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.

## 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 details:

- Associated Cisco CallManagers: The Associated Call Managers tab displays the details of all the Cisco CallManager servers associated with the selected gatekeeper device. The tab displays the details of every associated CallManager in the format presented in the [Cisco Call Manager view](#).
- Incidents: This tab displays the incidents generated based on the state of the GateKeeper.

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"><li>• Managed: indicates that the node is managed by the iSPI for IP Telephony.</li></ul>

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

## Monitoring Voice Gateways

The Voice Gateways view displays a list of available Cisco voice gateway devices in the network. The view arranges the key attributes of all discovered Cisco voice gateway devices in a table.

### To launch the Cisco Voice Gateways view

From the **Workspaces** navigation pane, click **Cisco IP Telephony > Voice Gateways**. The Cisco Voice Gateways view opens in the right pane.

### Basic Attributes of the Cisco Voice Gateway Table

Attribute	Description
Operational State	<p>The status of the Cisco voice gateway device. Possible values are:</p> <ul style="list-style-type: none"> <li>• No Status—the first polling cycle to collect the operational state has not taken place.</li> <li>• Normal—states of all associated circuit-switched interfaces with the voice gateway device are normal.</li> <li>• Unknown—states of all associated circuit-switched interfaces with the voice gateway device are unknown.</li> <li>• Warning—state of at least one associated circuit-switched interface is unknown; no associated circuit-switched interface is in the critical condition.</li> <li>• Minor—state of at least one (but not every) associated circuit-switched interface is critical.</li> <li>• Critical—state of every associated circuit-switched interface is critical.</li> <li>• Node Down—state of the voice gateway device is critical.</li> </ul>
Hosted Node	The hostname of the router on which the Cisco voice gateway device runs.
IP Address	The IP address of the Cisco voice gateway device.
Protocol	The protocol used by the gateway device.
Call Server	The fully-qualified domain name of the Cisco CallManager device to which the voice gateway device is configured.
Description	A description of the voice gateway device.

## Viewing Cisco Voice Gateway Endpoints


You can launch the Node form from the Voice Gateway view to view the endpoint details of a Cisco Voice Gateway device. The node form for a Cisco 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 endpoints of the Cisco Gateway device in a table.

#### To launch the Node form for a Cisco Voice Gateways device

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Voice Gateways**. The Voice Gateways view opens in the right pane.
2. In the right pane, click  within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.

Alternatively, follow these steps:

1. From the **Workspaces** navigation pane, click **Inventory > Nodes**. The Nodes view opens in the right pane. The Nodes view represents all the Cisco Voice Gateway devices (discovered by the iSPI for IP Telephony) as nodes.
2. In the right pane, click  within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.

After you launch the Node form for the Cisco Voice Gateway device, view the details of all the endpoints from the Voice Gateway Interfaces tab.

#### Node Form: Voice Gateway Interfaces Tab

The Voice Gateway Interfaces tab lists the key attributes of the endpoints of the Cisco Voice Gateway device.

#### Basic Attributes of the Voice Gateway Interfaces Tab



Attribute	Description
Registration State	Indicates if the endpoint is registered with a Cisco CallManager. This state is applicable only for interfaces with the Media Gateway Control Protocol (MGCP). Possible values are: <ul style="list-style-type: none"> <li>• Unknown</li> <li>• Registered</li> <li>• Unregistered</li> <li>• Rejected</li> <li>• Partially Registered</li> </ul>
Name	The host name of the endpoint.
Type	The type of the endpoint. Possible values are:
ifName	The name of the interface.
Usage State	The usage status of the endpoint. This state is not applicable for non-DS1 interfaces. Possible values are: <ul style="list-style-type: none"> <li>• Idle— if all channels associated with the interface are idle.</li> <li>• In-use—if all channels associated with the interface are in use.</li> <li>• Partially in-use—if at least one interface is in use (not all the interfaces are in use).</li> </ul>
Operational State	This field indicates the operational state of the endpoint. Possible values are:

Attribute	Description
	<ul style="list-style-type: none"> <li>• Up</li> <li>• Down</li> <li>• Testing</li> <li>• Unknown</li> <li>• Dormant</li> <li>• Not Present</li> <li>• Lower Layer Down</li> </ul>



### Viewing Cisco Voice Gateway Endpoint Channels

You can launch a Node form from the Voice Gateway Interfaces tab to view the channel details of an endpoint of a Cisco Voice Gateway device. This node form includes an additional tab—the **Voice Gateway Channels** tab. The Voice Gateway Channels tab arranges all the key attributes of all the channels of the Cisco Gateway device endpoint in a table.

#### To launch the Node form to view endpoint channel details of a Cisco Voice Gateway device

1. From the **Workspaces** navigation pane, click **Cisco IP Telephony > Voice Gateways**. The Voice Gateways view opens in the right pane.
2. In the right pane, click  within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.
3. In this form, click the **Voice Gateway Interfaces** tab. You can view a list of discovered endpoints.
4. Click  within the row representing the endpoint of your interest. The Node form opens. To view the channel details, click the **Voice Gateway Channels** tab.

Alternatively, follow these steps:

1. From the **Workspaces** navigation pane, click **Inventory > Nodes**. The Nodes view opens in the right pane. The Nodes view represents all the Cisco Voice Gateway devices (discovered by the iSPI for IP Telephony) as nodes along with the other general nodes.
2. In the right pane, click  within the row representing the Voice Gateway device of your interest. The Node form for the Cisco Voice Gateway device opens.
3. In this form, click the **Voice Gateway Interfaces** tab. You can view a list of discovered endpoints.
4. Click  within the row representing the endpoint of your interest. The Node form opens. To view the channel details, click the **Voice Gateway Channels** tab.

#### Node Form: Voice Gateway Channels Tab

The Circuit Switched Channels tab lists the key attributes of the channels (DS0) associated with the endpoints of the Cisco Voice Gateway device.

#### Basic Attributes of the Voice Gateway Channels Tab

Attribute	Description
Operational State	The operational state of the channel. Possible values are:

Attribute	Description
	<ul style="list-style-type: none"><li>• Up</li><li>• Down</li><li>• Testing</li><li>• Unknown</li><li>• Dormant</li><li>• Not present</li><li>• Lower layer down</li></ul>
Name	The name of the channel.
Type	The type of the channel.
ifName	The name of the interface.
Interface	The name of the associated interface.
Usage State	The usage state of the channel. Possible values are: <ul style="list-style-type: none"><li>• In-use</li><li>• Idle</li><li>• Unknown</li><li>• Not-pollled</li></ul>

## 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.
IP Address	Indicates the IP address of the device.
Version	Indicates the version of the 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.

## 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
Name	Indicates the name of device.
IP Address	Indicates the IP address of the device.
Version	Indicates the version of the device.

## 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](#).

## Monitoring Nortel Call Servers

The Call Servers view displays a list of available Nortel Call Servers in the network. The view arranges the key attributes of all discovered Nortel Call Servers in a table.

### To launch the Call Servers view

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

### Basic Attributes of the Nortel Call Servers Table

Attribute	Description
Node Status	The status of the Nortel Call Server. Possible values are: <ul style="list-style-type: none"><li>• No Status</li><li>• Normal</li></ul>




Attribute	Description
	<ul style="list-style-type: none"> <li>• Disabled</li> <li>• Warning</li> <li>• Minor</li> <li>• Major</li> <li>• Critical</li> <li>• Unknown</li> </ul>
Name	The system name of the Nortel Call Server.
IP Address	The IP address of the Nortel Call Server.
Model	The model of the Nortel Call Server.
Version	Version of the Nortel Call Server.
Description	A description of the Nortel Call Server.

### 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.

### 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.

Attribute	Description
Name	The name of the Nortel Call Server.
IP Address	The IP address of the Nortel Call Server.
Description	A short description of the server.
Version	The version of the server.
ELAN IP	IP address of the interface that is connected to the ELAN where the Nortel Call Server belongs.
Model	Model of the Nortel Call Server.

## Monitor Nortel Signaling Servers

The Signaling Servers view displays a list of available Nortel Signaling Servers in the network. The view arranges the key attributes of all discovered Nortel Signaling Servers in a table.

### To launch the Nortel Signaling Servers view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > Signaling Servers**. The Signaling Servers view opens in the right pane.


### Basic Attributes of the Nortel Signaling Servers Table


Attribute	Description
Node Status	The status of the Nortel Signaling Server. Possible values are: <ul style="list-style-type: none"> <li>• No Status</li> <li>• Normal</li> <li>• Disabled</li> <li>• Warning</li> <li>• Minor</li> <li>• Major</li> <li>• Critical</li> <li>• Unknown</li> </ul>
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.

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.

**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](#).
- **Incidents:** This tab displays the incidents related to the Signaling Server.

The left pane lists the following details of the selected Nortel Signaling Server:

**Basic Attributes of the Selected Nortel Signaling Server**

Attribute	Description
Hosted Node	The hostname of the Nortel Signaling Server node.
Name	The name of the Nortel Signaling Server.
IP Address	The IP address of the Nortel Signaling Server detected by NNMI.
Version	The version of the server.
Description	A short description of the server.
Model	Model of the Nortel Signaling Server.
ELANIpAddress	IP address of the interface that is connected to the ELAN where the Nortel Signaling Server belongs.
HostIpAddress	All the IP addresses of the Nortel Signaling Server.

**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.

### 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.

### 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](#).
- **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.

Attribute	Description
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.

## 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 ( <b>VGMC</b> ) and Media Gateway Controller ( <b>MGC</b> ).
Call Server	The fully-qualified domain name of the CS1000 server to which the gateway device is configured.
Protocol	The protocol used by the gateway device.
Description	A description of the media gateway device.

### 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.

## 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](#).
- **Incidents:** This tab displays the incidents related to the media gateway.

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.
Model	The model of the phone.
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.

## 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.

### To launch the Nortel QOS Zones table view

From the **Workspaces** navigation pane, click **Nortel IP Telephony > QOS Zones**. The QOS Zones table view opens in the right pane.


### 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.

### 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.

### 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.
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.

Attribute	Description
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.
WarnRFactorOut	The number of warning R-factor samples within different zones.
WarnEchoRLossOut	The number of warning Echo Return Loss within different 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](#).



## 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"><li>• Active—indicates the call controller is in the active state.</li><li>• Standby—indicates that the call controller is in the standby state.</li><li>• Unknown—indicates that the status of the call controller is currently unknown.</li></ul>
Name	Indicates the name of the call controller.
IP Address	Indicates the IP address of the call controller.
Type	Indicates the type of the call controller. The type can be one of the following: <ul style="list-style-type: none"><li>• Primary Server—indicates that the call controller is a primary server.</li><li>• LSP—indicates that the call controller is a Local Survivable Processor (LSP).</li></ul>
Version	Indicates the version of 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.

### Avaya Call Controller Details Form

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

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

- **Network Regions:** This tab displays the attributes of the configured network regions as shown in the [Monitoring Network Regions](#) page.
- **Route Patterns:** This tab displays the attributes of the configured route patterns as shown in the [Monitoring Route Patterns](#) page.
- **Trunk Groups:** This tab displays the details of the configured trunk groups as shown in the [Monitoring Trunk Groups](#) page.
- **Signaling Groups:** This tab displays the details of the configured signaling groups as shown in the [Monitoring Signaling Groups](#) page.
- **Occupancy:** This tab displays the call controller processor utilization metrics by different processes for the past one hour during which the processor utilization metrics were collected. You can specify threshold values for the different processes. as shown in the [Monitoring Processor Occupancy](#) page.
- **Media Gateways:** This tab displays the details of the media gateway associated with the call controller as shown in the [Monitoring Media Gateways](#) page.
- **Incidents:** This tab displays the incidents generated for the processes that violated the specified threshold.

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

**General Attributes of the Call Controller**

Attribute	Description
Hosted Node	The node on which the call controller is hosted.
Name	The name of the call controller.
IP Address	The IP address of the call controller.
Type	The type of the call controller.
Management Mode	Displays the management state of the Call Controller. The status can be one of the following strings: <ul style="list-style-type: none"> <li>• <b>Managed:</b> indicates that the node is managed by the iSPI for IP Telephony.</li> <li>• <b>Out of Service:</b> indicates that the node is currently out of service and not managed by the iSPI for IP Telephony.</li> <li>• <b>Unmanaged:</b> indicates that the node is currently not managed by the iSPI for IP Telephony.</li> </ul>
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.

Attribute	Description
Domain	The domain name of the call controller.
Location	The location of the call controller.

**Primary Server Attributes**

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

**Survivable Server Specific Attributes**

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

**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.

**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.
RSVP Profile	Lists the RSVP profile. The profile can be one of the following: <ul style="list-style-type: none"> <li>• controlled-load</li> <li>• guaranteed-service</li> </ul>
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.
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"><li>• Pass</li><li>• Fail</li></ul>
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"><li>• Direct</li><li>• Indirect</li></ul>
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 <b>Save and Close</b> icon from the menu to apply this threshold setting.
Transmit Bandwidth Used for Direct Connections	The transmit bandwidth used for direct connections

Attribute	Description
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.

### Route Pattern Detailed Form

The Route Pattern Detailed 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.
- Trunk Group Usage: displays the trunk group usage details as shown on the [Trunk Group Details Form](#) page.
- 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.

Attribute	Description
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"> <li>Managed: indicates that the route pattern is managed by the iSPI for IP Telephony.</li> <li>Out of Service: indicates that the route pattern is currently out of service and not managed by the iSPI for IP Telephony.</li> <li>Unmanaged: indicates that the route pattern is currently not managed by the iSPI for IP Telephony.</li> </ul>
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.
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 <b>Save and Close</b> 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.
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.

### 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.

Attribute	Description
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.

#### Usage Details of the Trunk Group

Attribute	Description
Total Seize	Indicates the number of times a trunk was seized in the group.
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.
Busy Group Members	Lists the number of busy trunk group members.
Free Group Members	Lists the number of free trunk group members.

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.

Attribute	Description
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.
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.

## 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.

Attribute	Description
-----------	-------------

### 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.

## 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"><li>• Registered</li><li>• Unregistered</li></ul>
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.
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.

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 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.

## 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, and Controller columns.

**To filter the Avaya IP Phones view:**

1. **Right-click the Registration State, Extension Number, IP Address, or Controller** attribute of one of the IP phones listed in the Avaya IP Phones view.
2. Select one of the following filters:
  - **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.
  - **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.

**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"> <li>• <b>Managed</b>: indicates that the IP Phone is managed by the iSPI for IP Telephony.</li> <li>• <b>Out of Service</b>: indicates that the IP Phone is currently out of service and not managed by the iSPI for IP Telephony.</li> <li>• <b>Unmanaged</b>: indicates that the IP Phone is currently not managed by the iSPI for IP Telephony.</li> </ul>
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.

Attribute	Description
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.

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

## Monitoring Avaya Port Networks

The Port Networks view displays a list of available port networks in the network. The view arranges the key attributes of all discovered Avaya port networks in a table.

### To launch the Port Networks view:

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


### 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: <ul style="list-style-type: none"> <li>In: denotes that the service state is active.</li> <li>Out: denotes that the service state is inactive.</li> </ul>
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"> <li>In: denotes that the service state is active.</li> <li>Out: denotes that the service state is inactive.</li> </ul>

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.

### 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.
- **IPSI:** 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
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"> <li>• In: denotes that the IPSI service is in the active state.</li> <li>• Out: denotes that the IPSI service is in the inactive state.</li> </ul>
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"> <li>• Active: indicates that the control state for the IPSI board is in the active state.</li> <li>• Standby: indicates that the control state for the IPSI board is in the Standby state.</li> </ul>

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.

## 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:

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

### 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

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	<p>Displays the management state of the CLAN. The status can be one of the following strings:</p> <ul style="list-style-type: none"> <li>• Managed: indicates that the CLAN is managed by the iSPI for IP Telephony.</li> <li>• Out of Service: indicates that the CLAN is currently out of service and not managed by the iSPI for IP Telephony.</li> <li>• Unmanaged: indicates that the CLAN is currently not managed by the iSPI for IP Telephony.</li> </ul>
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
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"> <li>Up: indicates that the link is up.</li> <li>Down: indicates that the link is down.</li> </ul>
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"> <li>Up: indicates that the link is up.</li> <li>Down: indicates that the link is down.</li> </ul>
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.

### 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	<p>Displays the management state of the media processor. The status can be one of the following strings:</p> <ul style="list-style-type: none"> <li>• Managed: indicates that the media processor is managed by the iSPI for IP Telephony.</li> <li>• Out of Service: indicates that the media processor is currently out of service and not managed by the iSPI for IP Telephony.</li> <li>• Unmanaged: indicates that the media processor is currently not managed by the iSPI for IP Telephony.</li> </ul>
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.
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"><li>• Active</li><li>• Standby</li><li>• Init</li></ul>
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.

## 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

## 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.

## 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.

## 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.

Metric	Description
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.

## 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.

## 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.

## 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.

## 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.

## 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.

## 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"> <li>Registered</li> <li>Unregistered</li> </ul>
Name	The name of the media gateway.
IP Address	The IP address of the media gateway.
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.

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.

### 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:

Attribute	Description
	<ul style="list-style-type: none"> <li>Managed: indicates that the media gateway is managed by the iSPI for IP Telephony.</li> <li>Out of Service: indicates that the media gateway is currently out of service and not managed by the iSPI for IP Telephony.</li> <li>Unmanaged: indicates that the media gateway is currently not managed by the iSPI for IP Telephony.</li> </ul>
Hardware Type	The hardware type of the media gateway.
Serial Number	The serial number of the media gateway.
Hardware Vintage	The hardware version of the media gateway.
Vintage Suffix	The vintage suffix of the media gateway.
Network Region	The network region to which the media gateway is associated.
Description	The description of the media gateway.
Default IP Address	The default IP address for the media gateway.
Gateway Number	The gateway number configured for the media gateway.
MAC Address	The MAC address of the media gateway.
Firmware Version	The firmware version of the media gateway.
Controller List	The controller list for the media gateway.
DHCP for IP Address	Indicates if DHCP is configured for the IP address.
DHCP for VLAN	Indicates if DHCP is configured for the VLAN.
DHCP for Controllers	Indicates if DHCP is configured for the call controllers.
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.

## 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"><li>• <b>Managed</b>: indicates that the media module is managed by the iSPI for IP Telephony.</li><li>• <b>Out of Service</b>: indicates that the media module is currently out of service and not managed by the iSPI for IP Telephony.</li><li>• <b>Unmanaged</b>: indicates that the media module is currently not managed by the iSPI for IP Telephony.</li></ul>
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.

Attribute	Description
Vintage Suffix	The vintage suffix of the media module.
Firmware Version	The firmware version of the media module.
Number of Ports	The number of ports on the media module.
Number of Channels.	The number of channels on the media module.

The **Faults** section displays the faults associated with the media module.

### Monitoring VOIP Engines


The VOIP Engines tab page displays the details specific to the VOIP engines associated with the media gateway. This page displays the following details.

#### Attributes of the VOIP Engines

Attribute	Description
Administrative State	Indicates the administrative state of the VOIP engine.
Faults Active	Specifies if this feature is enabled on the VOIP engine.
DSP State	Specifies the Digital Signal Processor (DSP) state on the VOIP engine.
ID	Lists the ID of the VOIP engine.
IP Address	Lists the IP address of the VOIP engine.

You can view the details of a single VOIP engine in a form.

#### To view the VOIP Engines form:

Select the VOIP engine of your interest, and then click . The VOIP Engines form opens.

## 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"> <li>• Managed: indicates that the VOIP engine is managed by the iSPI for IP</li> </ul>

Attribute	Description
	Telephony. <ul style="list-style-type: none"> <li>• Out of Service: indicates that the VOIP engine is currently out of service and not managed by the iSPI for IP Telephony.</li> <li>• Unmanaged: indicates that the VOIP engine is currently not managed by the iSPI for IP Telephony.</li> </ul>
MAC Address	The MAC address of the VOIP engine.
ID	The unique ID of the VOIP engine.
Default IP Address	The default IP address assigned to the VOIP engine.
Firmware Version	The firmware version of the VOIP engine.
Total Channels	The total number of channels on the VOIP engine.

#### State Attributes of the VOIP Engine

Attribute	Description
Administrative State	The administrative state of the VOIP engine.
DSP State	The DSP state of the VOIP engine.
Channels in Use	The number of channels in use on the VOIP engine.
Jitter Buffer Size	The buffer size allocated to jitter on the VOIP engine.
Hyperactivity Detected	Specifies whether hyperactivity is detected on the VOIP engine.
5-Minute Average Occupancy	Specifies the value for this parameter specified on the VOIP engine.

The **Faults** section lists the faults generated for the VOIP engine.

#### Monitoring DSP Cores

The DSP Cores tab page displays the details of the DSP cores associated with the media gateway. This page displays the following details.


#### Attributes of the DSP Cores

Attribute	Description
Administrative State	The administrative state of the DSP core.
DSP State	The state of the DSP core. the state can be one of the following: <ul style="list-style-type: none"> <li>• In Use:</li> <li>• Idle:</li> </ul>
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.

## 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"> <li>Managed: indicates that the DSP core is managed by the iSPI for IP Telephony.</li> <li>Out of Service: indicates that the DSP core is currently out of service and not managed by the iSPI for IP Telephony.</li> <li>Unmanaged: indicates that the DSP core is currently not managed by the iSPI for IP Telephony.</li> </ul>
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.

Incident	Message	Severity	Description
clarusipcPolicyTestTrap	\$1	Normal	This is a test SNMP policy trap.
clarusipcTaskInitiation	Task "\$1" initiated	Normal	An informational notification indicating the start of a ClarusIPC task. All other task-related notifications follow this incident.
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 iSPI for IP Telephony

When specific events occur in the IP telephony environment, the iSPI for IP Telephony sends incidents with appropriate messages to the NNMi incident view.

### Incidents Generated by the iSPI for IP Telephony

Cisco IP Telephony Incident	Message	Severity	Description
LowQOSCall	Low QOS Call: SRC Phone IP:\$origMediaIPAddress Extn:\$getCallingPartyNumber DEST Phone IP:\$destIPAddress Extn:\$finalCalledPartyNumber Cluster:\$getGlobalCallId_ ClusterId Jitter:\$jitter Latency:\$latency MOS:\$avgMLQK	Critical	This incident indicates a low voice quality call between two given phone numbers along with their extension and IP address details, cluster-Id of the source phone number and QoS details (such as Jitter, Latency, and average MOS).
CiscoCktSwitchedIFStatusIdle	Cisco Ckt Switched interface changed usage status to idle. Gateway ipaddress : \$gwIPAddress	Warning	This incident indicates that the usage state of a circuit switched interface i.e. 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 bearer channels for the endpoint.
CiscoCktSwitchedIFOperStatusDown	The operational state of a Cisco Ckt Switched interface has changed to critical. Gateway ipaddress : \$gwIPAddress	Critical	This incident indicates that the operational state of a circuit switched interface (endpoint) hosted on a voice gateway has changed from up to down. The operational state of an endpoint is computed by considering the operational states of the endpoint and bearer channels for the endpoint.
CiscoCktSwitchedChannelStatusIdle	Cisco Circuit Switched Channel changed usage status to Idle.	Critical	This incident indicates that a Cisco circuit switched

Cisco IP Telephony Incident	Message	Severity	Description
CiscoCktSwitchedChannelOperStatusDown	The operation state of a Cisco Ckt Switched channel has changed to critical.	Critical	channel that its u is now i  This indicates the operational status of the circuit switched channel has changed to critical.
CiscoCallManagerStatusDown	Call Manager Down. IP: \$ip Cluster: \$cluster	Critical	Call Manager Down
CiscoCktSwitchedIFRegnStatusUnReg	The registration state of a Cisco Ckt Switched interface has changed to critical. Gateway ipaddress : \$gwIPAddress	Critical	This indicates the registration status of the circuit switched interface (either hosted or gateway) has changed to critical. It happens when the registered to unregistered.
CiscoCktSwitchedIFRegnStatusRejected	The registration state of a Cisco Ckt Switched interface has changed to critical. Gateway ipaddress : \$gwIPAddress	Critical	This indicates the registration status of the circuit switched interface (either hosted or gateway) has changed to critical. It happens when the call manager rejects an interface registration request.
CiscoCktSwitchedIFRegnStatusUnknown	The registration state of Cisco circuit switched interface : \$cktSwIFName has changed to unknown. Gateway ipaddress : \$gwIPAddress	Critical	This indicates the registration status of the circuit switched interface (either hosted or gateway) has changed to unknown.
CiscoPhoneUnRegistered	Cisco Phone Unregistered from CallManager.	Minor	Cisco Phone Unregistered from CallManager
CiscoPhoneUnknown	Cisco Phone registration status is not known	Minor	Cisco Phone registration status is not known.

Cisco IP Telephony Incident	Message	Severity	Description
CiscoPhoneDeceased	Cisco Phone Deceased Extn: \$extn IP Address: \$ip CallController: \$csIPAddress MAC: \$mac Cluster: \$cluster	Warning	The Cisco IP Phone configured to register with the SRST in back mode has deceased
CiscoPhonePartiallyRegistered	Cisco Phone has some extensions unregistered.	Warning	Cisco Phone has some extensions unregistered.
CiscoSrstActive	Cisco Srst Active: \$ip	Critical	The Cisco SRST is in the active state.
CiscoVMDeviceRejected	Cisco Voice Mail Device \$vmName, with IP Address: \$ipAddress, Controller: \$ccmIPAddress, has changed its state to Rejected.	Critical	The Cisco Voice Mail Device has changed its state to Rejected.
CiscoVMDeviceUnknown	Cisco Voice Mail Device \$vmName, with IP Address: \$ipAddress, Controller: \$ccmIPAddress, has changed its state to Unknown.	Critical	The Cisco Voice Mail Device has changed its state to Unknown.
CiscoVMDeviceUnregistered	Cisco Voice Mail Device \$vmName, with IP Address: \$ipAddress has Unregistered from \$ccmIPAddress	Minor	The Cisco VM Device is in the unregistered state.
CiscoGkControlledICTStatusRejected	The Gatekeeper-Controlled Inter-Cluster Trunk has changed its registration state to Rejected. Call Manager IP: \$cmIPAddress	Critical	This incident is generated whenever a Gatekeeper-Controlled Inter-Cluster Trunk's registration request is rejected by a Cisco Call-Manager.
CiscoGkControlledICTStatusUnRegd	The Gatekeeper-Controlled Inter-Cluster Trunk has changed its registration state to UnRegistered.	Critical	This incident is generated when even a Gatekeeper-Controlled Inter-Cluster Trunk unregisters 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.
Nortel IP Telephony Incident	Message	Severity	Description
callsMadeInViolation	The Intra QOS Zone callsMadeIn parameter has violated set threshold value.	Critical	The Intra QOS Zone callsMadeIn parameter has violated threshold value.

Cisco IP Telephony Incident	Message	Severity	Description
callsMadeOutViolation	The Inter QOS Zone callsMadeOut parameter has violated set threshold value.	Critical	The Inter callsMadeOut parameter has violated set threshold value.
callsBlockedOutViolated	The Inter QOS Zone callsBlockedOut parameter has violated set threshold value.	Critical	The Inter callsBlockedOut parameter has violated set threshold value.
callsPeakInViolated	The Intra QOS Zone peakIn parameter has violated set threshold value.	Critical	The Intra peakIn parameter has violated set threshold value.
callsBlockedInViolated	The Intra QOS Zone callsBlockedIn parameter has violated set threshold value.	Critical	The Intra callsBlockedIn parameter has violated set threshold value.
callsPeakOutViolated	The Inter QOS Zone peakOut parameter has violated set threshold value.	Critical	The Inter peakOut parameter has violated set threshold value.
inThrViolViolated	The Intra QOS Zone inThrViol parameter has violated set threshold value.	Critical	The Intra inThrViol parameter has violated set threshold value.
outThrViolViolated	The Inter QOS Zone outThrViol parameter has violated set threshold value.	Critical	The Inter outThrViol parameter has violated set threshold value.
avgInViolated	The Intra QOS Zone avgIn parameter has violated set threshold value.	Critical	The Intra avgIn parameter has violated set threshold value.
avgOutViolated	The Inter QOS Zone avgOut parameter has violated set threshold value.	Critical	The Inter avgOut parameter has violated set threshold value.
unacpLatencyInViolated	The Intra QOS Zone unacpLatencyIn parameter has violated set threshold value.	Critical	The Intra unacpLatencyIn parameter has violated set threshold value.
intervalOutViolated	The Inter QOS Zone intervalOut parameter has violated set threshold value.	Critical	The Inter intervalOut parameter has violated set threshold value.

Cisco IP Telephony Incident	Message	Severity	Description
			eter has violated threshold value.
intervallnViolated	The Intra QOS Zone intervalln parameter has violated set threshold value.	Critical	The Intra QOS Zone intervalln 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 violated set threshold value.	Critical	The Intra QOS Zone unacpJitterIn parameter has violated set threshold value.
unacpRFactorOutViolated	The Inter QOS Zone unacpRFactorOut parameter has violated set threshold value.	Critical	The Inter QOS Zone unacpRFactorOut parameter has violated set threshold value.
unacpEchoRLossOutViolated	The Inter QOS Zone unacpEchoRLossOut parameter has violated set threshold value	Critical	The Inter QOS Zone unacpEchoRLossOut parameter has violated set threshold value.

Cisco IP Telephony Incident	Message	Severity	Description
unacpEchoRLossInViolated	The Intra QOS Zone unacpEchoRLossIn parameter has violated set threshold value.	Critical	The Intra unacpEchoRLossIn parameter has violated set threshold value.
warnPacketLossInViolated	The Intra QOS Zone warnPacketLossIn parameter has violated set threshold value.	Critical	The Intra warnPacketLossIn parameter has violated set threshold value.
warnLatencyOutViolated	The Inter QOS Zone warnLatencyOut parameter has violated set threshold value.	Critical	The Inter warnLatencyOut parameter has violated set threshold value.
warnLatencyInViolated	The Intra QOS Zone warnLatencyIn parameter has violated set threshold value.	Critical	The Intra warnLatencyIn parameter has violated set threshold value.
warnRFactorInViolated	The Intra QOS Zone warnRFactorIn parameter has violated set threshold value.	Critical	The Intra warnRFactorIn parameter has violated set threshold value.
warnJitterOutViolated	The Inter QOS Zone warnJitterOut parameter has violated set threshold value.	Critical	The Inter warnJitterOut parameter has violated set threshold value.
warnEchoRLossInViolated	The Intra QOS Zone warnEchoRLossIn parameter has violated set threshold value.	Critical	The Intra warnEchoRLossIn parameter has violated set threshold value.
warnEchoRLossOutViolated	The Inter QOS Zone warnEchoRLossOut parameter has violated set threshold value.	Critical	The Inter warnEchoRLossOut parameter has violated set threshold value.
warnRFactorOutViolated	The Inter QOS Zone warnRFactorOut parameter has violated set threshold value.	Critical	The Inter warnRFactorOut parameter has violated set threshold value.
warnJitterInViolated	The Intra QOS Zone warnJitterIn parameter has violated set threshold value.	Critical	The Intra warnJitterIn parameter has violated set threshold value.



Cisco IP Telephony Incident	Message	Severity	Description
			eter has violated 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.
NortelSetStatusUnregistered	Nortel IP Phone Unregistered. Extension: \$extension. Signaling Server: \$sslpAddress. 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 the VARIABLES clause are defined in the mgmt-info group and are present in all information alarms.
commonMIBAlarmCritical	Critical alarm condition on Nortel device \$6. Err Code \$7. Alarm Type \$8. Probable Cause \$9. Alarm Data \$10.	Critical	This trap is used to provide a real time indication of a critical alarm condition. The variables listed in the VARIABLES clause are defined in the mgmt-info group and are present in all information alarms.
commonMIBAlarmClear	Clear alarm condition on Nortel device \$6. Err Code \$7. Alarm Type \$8. Probable Cause \$9. Alarm Data \$10.	Normal	This trap is used to provide a real time indication of a clear alarm condition. The variables listed in the VARIABLES clause are defined in the mgmt-info 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 the VARIABLES clause are defined in the mgmt-info group and

Cisco IP Telephony Incident	Message	Severity	Description
commonMIBAlarmInfo	Informational alarm condition on Nortel device \$6. Err Code \$7. Alarm Type \$8. Probable Cause \$9. Alarm Data \$10.	Normal	This trap provides information and indication of an informational alarm condition. The alarm condition is listed in clause a) of the mgmt-iSPI and are informational.
commonMIBAlarmMajor	Major alarm condition on Nortel device \$6. Err Code \$7. Alarm Type \$8. Probable Cause \$9. Alarm Data \$10.	Major	This trap provides information and indication of a major alarm condition. The alarm condition is listed in clause a) of the mgmt-iSPI and are informational.
commonMIBAlarmWarning	Warning alarm condition on Nortel device \$6. Err Code \$7. Alarm Type \$8. Probable Cause \$9. Alarm Data \$10.	Warning	This trap provides information and indication of a warning alarm condition. The alarm condition is listed in clause a) of the mgmt-iSPI and are informational.
Avaya IP Telephony Incident	Message	Severity	Description
AvayaECCStatusActive	Paired Avaya Primary Server is in active state. IP Address : \$ipAddress	Normal	The paired Avaya Primary Server is in active state.
AvayaECCStatusBusyout	Paired Avaya Primary Server is in busyout state. IP Address : \$ipAddress	Normal	The paired Avaya Primary Server is in busyout state.
AvayaECCStatusDormant	Paired Avaya Primary Server is in dormant state. IP Address : \$ipAddress	Normal	The paired Avaya Primary Server is in dormant state.
AvayaECCStatusStandby	Paired Avaya Primary Server is in standby state. IP Address : \$ipAddress	Normal	The paired Avaya Primary Server is in standby state.

Cisco IP Telephony Incident	Message	Severity	Description
AvayaInclncomingPegViolate	Avaya Port Network, Incoming Trunk Load, Incoming Peg parameter breached threshold, PN Name: \$number, Value: \$loadinclncomingPeg, Threshold: \$loadinclncomingPegThreshold	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
AvayaInclncomingUseViolate	Avaya Port Network, Incoming Trunk Load, Incoming Use parameter breached threshold, PN Name: \$number, Value: \$loadinclncomingUse, Threshold: \$loadinclncomingUseThreshold	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
AvayaInclntraPNPegViolate	Avaya Port Network, Incoming Trunk Load, Intra PN Peg parameter breached threshold, PN Name: \$number, Value: \$loadinclntraPNPeg, Threshold: \$loadinclntraPNPegThreshold	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
AvayaInclntraPNUseViolate	Avaya Port Network, Incoming Trunk Load, Intra PN Use parameter breached threshold, PN Name: \$number, Value: \$loadinclntraPNUse, Threshold: \$loadinclntraPNUseThreshold	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
AvayaInclncOutgoingPegViolate	Avaya Port Network, Incoming Trunk Load, Outgoing Peg parameter breached threshold, PN Name: \$number, Value: \$loadinclncOutgoingPeg, Threshold: \$loadinclncOutgoingPegThreshold	Warning	This incident is generated when the Incoming Trunk Load, Outgoing Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network.

Cisco IP Telephony Incident	Message	Severity	Description
AvayaIncOutgoingUseViolate	Avaya Port Network, Incoming Trunk Load, Outgoing Use parameter breached threshold, PN Name: \$number, Value: \$loadinIncOutgoingUse, Threshold: \$loadinIncOutgoingUseThreshold	Warning	This incident was generated by Avaya Port Network. Incoming Trunk Load, Outgoing Use parameter breached threshold. Please check the configuration of the Avaya Port Network.
AvayaIntInterPNPegViolate	Avaya Port Network, Intercom Inter PN Peg parameter breached threshold, PN Name: \$number, Value: \$loadintIntInterPNPeg, Threshold: \$loadintIntInterPNPegThreshold	Warning	This incident was generated by Avaya Port Network. Intercom Inter PN Peg parameter breached threshold. Please check the configuration of the Avaya Port Network.
AvayaIntInterPNUseViolate	Avaya Port Network, Intercom Inter PN Use parameter breached threshold, PN Name: \$number, Value: \$loadintIntInterPNUse, Threshold: \$loadintIntInterPNUseThreshold	Warning	This incident was generated by Avaya Port Network. Intercom Inter PN Use parameter breached threshold. Please check the configuration of the Avaya Port Network.
AvayaIntIntraPNPegViolate	Avaya Port Network, Intercom Intra PN Peg parameter breached threshold, PN Name: \$number, Value: \$loadintIntIntraPNPeg, Threshold: \$loadintIntIntraPNPegThreshold	Warning	This incident was generated by Avaya Port Network. Intercom Intra PN Peg parameter breached threshold. Please check the configuration of the Avaya Port Network.
AvayaIntIntraPNUseViolate	Avaya Port Network, Intercom Intra PN Use parameter breached threshold, PN Name: \$number, Value: \$loadintIntIntraPNUse, Threshold: \$loadintIntIntraPNUseThreshold	Warning	This incident was generated by Avaya Port Network. Intercom Intra PN Use parameter breached threshold. Please check the configuration of the Avaya Port Network.
AvayaMGwModuleStatusFaultActive	Fault Active on media module number \$slotNumber of Avaya Media Gateway \$gatewayIpAddress.	Warning	The Avaya Media Gateway module is in Active state.

Cisco IP Telephony Incident	Message	Severity	Description
AvayaMGwStatusUnregistered	Avaya Media Gateway Unregistered. IP Address: \$ipAddress.	Critical	The Avaya Media Gateway is in the Unregistered sta
AvayaMGwVoIPEngineStatusFaultActive	Fault Active on Avaya VoIP Engine Id \$slotNumber of Avaya Media Gateway \$gatewayIpAddress.	Warning	The VoIP Engine in the Fault Active status.
AvayaOutIncomingPegViolate	Avaya Port Network, Outgoing Trunk Load, Incoming Peg parameter breached threshold, PN Name: \$number, Value: \$loadoutOutIncomingPeg, Threshold: \$loadoutOutIncomingPegThreshold	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	Avaya Port Network, Outgoing Trunk Load, Incoming Use parameter breached threshold, PN Name: \$number, Value: \$loadoutOutIncomingUse, Threshold: \$loadoutOutIncomingUseThreshold	Warning	This incident is generated when the outgoing Trunk Load Incoming Use Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaOutIntraPNPegViolate	Avaya Port Network, Outgoing Trunk Load, Intra PN Peg parameter breached threshold, PN Name: \$number, Value: \$loadoutOutIntraPNPeg, Threshold: \$loadoutOutIntraPNPegThreshold	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	Avaya Port Network, Outgoing Trunk Load, Intra PN Use parameter breached threshold, PN Name: \$number, Value: \$loadoutOutIntraPNUse, Threshold: \$loadoutOutIntraPNUseThreshold	Warning	This incident is generated when the outgoing Trunk Load Intra PN Use Parameter in Avaya Port Network, has breached the threshold you specified for Avaya Port Network
AvayaOutOutgoingPegViolate	Avaya Port Network, Outgoing Trunk Load, Outgoing Peg parameter breached threshold, PN Name: \$number, Value: \$loadoutOutOutgoingPeg, Threshold: \$loadoutOutOutgoingPegThreshold	Warning	This incident is generated when the outgoing Trunk Load

Cisco IP Telephony Incident	Message	Severity	Description
			Outgoing parameter in Avaya Port Network has breached threshold, PN Name: \$number, Value: \$loadoutOutOutgoingUse, Threshold: \$loadoutOutOutgoingUseThreshold
AvayaOutOutgoingUseViolate	Avaya Port Network, Outgoing Trunk Load, Outgoing Use parameter breached threshold, PN Name: \$number, Value: \$loadoutOutOutgoingUse, Threshold: \$loadoutOutOutgoingUseThreshold	Warning	This incident was generated by Avaya Port Network. Outgoing Trunk Load parameter in Avaya Port Network has breached threshold, PN Name: \$number, Value: \$loadoutOutOutgoingUse, Threshold: \$loadoutOutOutgoingUseThreshold
AvayaPNOccViolate	Avaya Port Network, PN Link Occupancy parameter breached threshold, PN Name: \$number, Value: \$loadtotalPNOccupancy, Threshold: \$loadtotalPNOccupancyThreshold	Warning	This incident was generated by Avaya Port Network. Link Occupancy parameter in Avaya Port Network has breached threshold, PN Name: \$number, Value: \$loadtotalPNOccupancy, Threshold: \$loadtotalPNOccupancyThreshold
AvayaPhoneUnknown	Avaya Phone with Extn: \$extn IP Address: \$ipAddress Controller: \$controllerIPAddress, has changed its state to Unknown.	Critical	The Avaya Phone with Extn: \$extn IP Address: \$ipAddress Controller: \$controllerIPAddress has changed its state to Unknown.
AvayaPhoneUnregistered	Avaya Phone Unregistered Extn: \$extn IP Address: \$ipAddress Controller: \$controllerIPAddress	Minor	The Avaya Phone Unregistered Extn: \$extn IP Address: \$ipAddress Controller: \$controllerIPAddress is unregistered.
AvayaRPQueOvflowThreVio	Queue Overflow threshold violated for Avaya Route Pattern: \$rpNumber on Hosted Node: \$hostNodeIP. Configured threshold value: \$queueOvflowThrVal, violated value: \$queueOvflow.	Warning	Queue Overflow threshold violated for Avaya Route Pattern: \$rpNumber on Hosted Node: \$hostNodeIP. Configured threshold value: \$queueOvflowThrVal, violated value: \$queueOvflow.
AvayaSGServiceStatusOut	Avaya Signaling Group: \$sgNumber on Call Controller \$hostNodeIP has become out of service.	Critical	Avaya Signaling Group: \$sgNumber on Call Controller \$hostNodeIP has become out of service.
AvayaSuServerStatusActive	Avaya Survivable Server(\$type) with IP Address: \$ipAddress has changed its state to active to provide local survivability to endpoints registered with Primary Controller: \$primaryIP	Critical	Avaya Survivable Server(\$type) with IP Address: \$ipAddress has changed its state to active to provide local survivability to endpoints registered with Primary Controller: \$primaryIP
AvayaSuServerStatusStandby	Avaya Survivable Server(\$type) with IP Address: \$ipAddress has changed its state to standby	Normal	Avaya Survivable Server(\$type) with IP Address: \$ipAddress has changed its state to standby

Cisco IP Telephony Incident	Message	Severity	Description
AvayaTMServiceStatusOutFE	Avaya Group Member: \$tmNumber of Trunk Group \$tgNumber on Call Controller: \$hostNodeIP has become out of service (far-end).	Critical	its state to standb Avaya Group Member has become out of service (far-end).
AvayaTMServiceStatusOutNE	Avaya Group Member: \$tmNumber of Trunk Group \$tgNumber on Call Controller: \$hostNodeIP has become out of service (near-end).	Critical	Avaya Group Member has become out of service (near-end).
AvayaTanIncomingPegViolate	Avaya Port Network, Tandem Trunk Load, Incoming Peg parameter breached threshold, PN Name: \$number, Value: \$loadtanTanIncomingPeg, Threshold: \$loadtanTanIncomingPegThreshold	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	Avaya Port Network, Tandem Trunk Load, Incoming Use parameter breached threshold, PN Name: \$number, Value: \$loadtanTanIncomingUse, Threshold: \$loadtanTanIncomingUseThreshold	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	Avaya Port Network, Tandem Trunk Load, Intra PN Peg parameter breached threshold, PN Name: \$number, Value: \$loadtanTanIntraPNPeg, Threshold: \$loadtanTanIntraPNPegThreshold	Warning	This incident is generated when the Tandem Trunk Load, Intra PN Peg Parameter in Avaya Port Network, has breached the threshold you specified for an Avaya Port Network
AvayaTanIntraPNUseViolate	Avaya Port Network, Tandem Trunk Load, Intra PN Use parameter breached threshold, PN Name: \$number, Value: \$loadtanTanIntraPNUse, Threshold: \$loadtanTanIntraPNUseThreshold	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

Cisco IP Telephony Incident	Message	Severity	Description
AvayaTanOutgoingPegViolate	Avaya Port Network, Tandem Trunk Load, Outgoing Peg parameter breached threshold, PN Name: \$number, Value: \$loadtanTanOutgoingPeg, Threshold: \$loadtanTanOutgoingPegThreshold	Warning	This incident was generated when the Tandem Trunk Load Outgoing Peg parameter in Avaya Port Network breached threshold. Would you like to view an Avaya work
AvayaTanOutgoingUseViolate	Avaya Port Network, Tandem Trunk Load, Outgoing Use parameter breached threshold, PN Name: \$number, Value: \$loadtanTanOutgoingUse, Threshold: \$loadtanTanOutgoingUseThreshold	Warning	This incident was generated when the Tandem Trunk Load Outgoing Use parameter in Avaya Port Network breached threshold. Would you like to view an Avaya work
AvayaTotalTDMOccViolate	Avaya Port Network, TDM Occupancy parameter breached threshold, PN Name: \$number, Value: \$loadtotalTDMOccupancy, Threshold: \$loadtotalTDMOccupancyThreshold	Warning	This incident was generated when the TDM Occupancy Parameter in Avaya Port Network breached threshold. Would you like to view an Avaya work.
avayaMedProUnknown	The Avaya Media Processor is in Unknown state	Warning	The Avaya Media Processor is in Unknown state
avayaMedProStandby	The Avaya Media Processor is in Standby state	Warning	The Avaya Media Processor is in Standby state
avayaMedProInit	The Avaya Media Processor is in Init state	Warning	The Avaya Media Processor is in Init state
avayaMedProControlLinkUnknown	The Avaya Media Processor Control Link is in Unknown state	Warning	The Avaya Media Processor Control Link is in Unknown state
avayaMedProControlLinkDown	The Avaya Media Processor Control Link is in Down state	Critical	The Avaya Media Processor Control Link is in Down state



Cisco IP Telephony Incident	Message	Severity	Description
			state
avayaIPServerInterfaceUnknown	The Avaya IP Server Interface (IPSI) Service State is in Unknown state	Warning	The Avaya IP Server Interface (IPSI) Service State is in the Unknown state
avayaIPServerInterfaceOUT	The Avaya IP Server Interface (IPSI) Service State is in OUT state	Critical	The Avaya IP Server Interface (IPSI) Service State is in OUT state
avayaIPNetworkRegionConnectionViolate	Avaya IP Network Region Denial Connection Count breached threshold, Source: \$source and Destination: \$destination, Value: \$denialCount, Threshold: \$threshold	Critical	The Avaya IP Network Region Denial Connection Count breached the threshold.
avayaIPNetworkRegionConnectionUnknown	Avaya IP Network Region Connection Status, between \$source and \$destination is in Unknown state	Warning	The Avaya IP Network Region Connection Status, between \$source and \$destination is in the Unknown state
avayaIPNetworkRegionConnectionFail	Avaya IP Network Region Connection, between \$source and \$destination is in Failed state	Critical	Avaya IP Network Region Connection between source and destination is in the Failed state
ProcTotalCallsViolate	Processor Total Calls Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor Total Calls Occupancy has breached the threshold specified by you on the Avaya Media Server
ProcTotalAttemptedCallsViolate	Processor Total Call Attempts Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	Processor Total Call Attempts Occupancy has breached the threshold specified by you on the Avaya Media Server.
ProcTandemCallsViolate	Processor Tandem Calls Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor Tandem Calls Occupancy has breached the threshold specified by you on the Avaya Media Server
ProcSystemMgmtViolate	Processor System Management Processing Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor System Management Processing Occupancy has breached

Cisco IP Telephony Incident	Message	Severity	Description
ProcStaticOccuViolate	Processor Static Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor Static Occupancy has breached user set threshold on the Avaya Media Server.
ProcPrivNetAttemptsViolate	Processor Private Network Attempts Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor Private Network Attempts Occupancy has breached user set threshold on the Avaya Media Server.
ProcOutCallsViolate	Processor Outgoing Attempts Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor Outgoing Attempts Occupancy has breached user set threshold on the Avaya Media Server.
ProcIntercomCallsViolate	Processor Intercom Attempts Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor Intercom Attempts Occupancy has breached user set threshold on the Avaya Media Server.
ProcIncomingCallsViolate	Processor Incoming Call Attempts Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor Incoming Call Attempts Occupancy has breached user set threshold on the Avaya Media Server.
ProcIdleOccupancyViolate	Processor Idle Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor Idle Occupancy has breached user set threshold on the Avaya Media Server.
ProcCallProcessingViolate	Processor Call Processing Occupancy has breached user set threshold on Avaya Media Server \$ipAddress, Current value: \$currentValue and Threshold value: \$thresholdVal	Warning	The Processor Call Processing Occupancy has breached user set threshold on the Avaya Media Server.

Cisco IP Telephony Incident	Message	Severity	Description
IPNetworkRegionUsageViolate	Avaya IP Media Processor DSP Resource Usage Parameter breached threshold, Current Value: \$ipdspUsage, Threshold set: \$ipdspUsageThreshold in Region: \$number	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource Usage parameter has breached the threshold value you specified for an IP Network Region.
IPNetworkRegionPercentBlockedViolate	Avaya IP Media Processor DSP Resource Allocations Blocked Percentage Parameter breached threshold, Current Value: \$pctBlocked, Threshold set: \$pctBlockedThreshold in Region: \$number	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	Avaya IP Media Processor DSP Resource Percentage of Out Of Service Parameter breached threshold, Current Value: \$outOfSrv, Threshold set: \$outOfSrvThreshold in Region: \$number	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	Avaya IP Media Processor DSP Resource G723 Usage parameter breached threshold, Current Value: \$codecG723Usage, Threshold set: \$codecG723UsageThreshold in Region: \$number	Warning	This incident is generated when the G723 Usage Parameter in Avaya IP Media Processor DSP Resource has breached the threshold value you specified for an IP Network Region.
IPNetworkRegionG723OutViolate	Avaya IP Media Processor DSP Resource G723 Out Of Region Allocations Parameter breached threshold, Current Value: \$codecG723OutRegion, Threshold set: \$codecG723OutRegionThreshold in Region: \$number	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.

Cisco IP Telephony Incident	Message	Severity	Description
IPNetworkRegionG723InViolate	Avaya IP Media Processor DSP Resource G723 InRegion Allocations Parameter breached threshold, Current Value: \$codecG723InRegion, Threshold set: \$codecG723InRegionThreshold in Region: \$number	Warning	This incident was generated by Avaya IP Media Processor DSP Resource G723 InRegion Allocations parameter has breached threshold specified for Network
IPNetworkRegionG711UsageViolate	Avaya IP Media Processor DSP Resource G711 Usage parameter breached threshold, Current Value: \$codecG711Usage, Threshold set: \$codecG711UsageThreshold in Region: \$number	Warning	This incident was generated by Avaya IP Media Processor DSP Resource G711 Usage parameter has breached threshold specified for Network
IPNetworkRegionG711OutViolate	Avaya IP Media Processor DSP Resource G711 Out Of Region Allocations Parameter breached threshold, Current Value: \$codecG711OutRegion, Threshold set: \$codecG711OutRegionThreshold in Region: \$number	Warning	This incident was generated by Avaya IP Media Processor DSP Resource G711 Out Of Region Allocations parameter has breached threshold specified for Network
IPNetworkRegionG711InViolate	Avaya IP Media Processor DSP Resource G711 InRegion Allocations parameter breached threshold, Current Value: \$codecG711InRegion, Threshold set: \$codecG711InRegionThreshold in Region: \$number	Warning	This incident was generated by Avaya IP Media Processor DSP Resource G711 InRegion Allocations parameter has breached threshold specified for Network
IPNetworkRegionDeniedViolate	Avaya IP Media Processor DSP Resource Allocations Denied Parameter breached threshold, Current Value: \$dspDenied, Threshold set: \$dspDeniedThreshold in Region: \$number	Warning	This incident was generated by Avaya IP Media Processor DSP Resource Allocations Denied parameter has breached threshold specified for Network

Cisco IP Telephony Incident	Message	Severity	Description
IPNetworkRegionDSPOutViolate	Avaya IP Media Processor DSP Resource Out of Region Allocations Parameter breached threshold, Current Value: \$dspOutRegion, Threshold set: \$dspOutRegionThreshold in Region: \$number	Warning	Network Region. 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	Avaya IP Media Processor DSP Resource InRegion Allocations Parameter breached threshold, Current Value: \$dspInRegion, Threshold set: \$dspInRegionThreshold in Region: \$number	Warning	This incident is generated when the Avaya IP Media Processor DSP Resource In Region Allocations parameter has breached the threshold value you specified for an IP Network Region.

## Viewing the Network Connectivity

With the 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 an operator (level 1 or level 2) or guest credential, 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.

The iSPI for IP Telephony presents three additional views—**Voice Path**, **Control Path**, and the **HTTP to Phone Path**—that help you construct the connecting path between two different IP phones (voice path) or between an IP phone and the call controller with which the phone is registered (control path). The HTTP to

Phone Path view provides you the details regarding the configuration of the IP phone. You can launch this view only for the Cisco IP 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.

### 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 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.

### 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 *HP NNM i Software 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.

## Reference Information

This section includes reference information on the processes and commands presented by the iSPI for IP Telephony. The iSPI for IP Telephony introduces the **encryptiptpasswd.ovpl** command and the **iptjboss** process.

This section includes the following topics:

- [iptjboss](#)
- [encryptiptpasswd.ovpl](#)

### Name

**iptjboss**—This is a customized version of the jboss application server for the HP NNM i Software Smart Plug-in for IP Telephony (iSPI for IP Telephony).

### Synopsis

iptjboss

### DESCRIPTION

iptjboss is managed by ovspmd. It uses the \$NNM\_DATA/shared/ipt/conf/nms-ipt.jvm.properties file to pass arguments to the iSPI for IP Telephony jboss application server.

You can start it by running **ovstart** or **ovstart -c iptjboss**. To stop it, run **ovstop** or **ovstop -c iptjboss**. To see the status of it, run **ovstatus -c iptjboss** or **ovstatus -v iptjboss**.

The **iptjboss** process starts and stops along with NNMi processes. The **iptjboss** process hosts all the iSPI for IP Telephony services including discovery, polling, GUI server, and so on.

If there are problems starting iptjboss, see the \$NNM\_DATA/log/ipt/jbossServer.log file and other log files present in the \$NNM\_DATA/log/ipt directory for more information. The iptjboss process determines the trace level from the \$NNM\_DATA/shared/ipt/conf/logging.properties file for logging data in the log files present in the \$NNM\_DATA/log/ipt directory. For more information, see the online help.

### EXAMPLES

To start the **iptjboss** processes along with other NNMi processes, run the following command:

```
$InstallDir/bin/ovstart
```

To start only the **iptjboss** process, run the following command:

```
$InstallDir/bin/ovstart -c iptjboss
```

To find the status of the **iptjboss** process, run the following command:

```
$InstallDir/bin/ovstatus -c iptjboss
```

### AUTHOR

**iptjboss** was developed by Hewlett-Packard Company.



## FILES

The **iptjboss** process uses the following parameter files:

<b>\$NNM_</b> <b>DATA/shared/ipt/conf/nms-</b> <b>ipt.jvm.properties</b>	This file contains the parameters that are passed to the JVM where iptjboss runs.
<b>\$NNM_</b> <b>DATA/shared/ipt/conf/nms-</b> <b>ipt.ports.properties</b>	This file contains the lists of ports used by iptjboss.
<b>\$NNM_DATA/log/ipt/jboss-</b> <b>Server.log</b>	This file contains the exceptions generated by iptjboss.

## Name

**encryptiptpasswd.ovpl**—This command updates the HP NNM i Software Smart Plug-in for IP Telephony (iSPI for IP Telephony) jboss application server with the modified NNMi system account password and modifies the Web Server Client password (used during the iSPI for IP Telephony installation).

## Synopsis

**encryptiptpasswd.ovpl -c ipt**

**encryptiptpasswd.ovpl -e ipt <new-password>**

## DESCRIPTION

If you change the NNMi system account password after installing the iSPI for IP Telephony, you must update the iSPI for IP Telephony jboss application server with the changed password using this command. The password is stored in an encrypted format.

You can use this command to modify the password of the Web Service Client user, which was used during the iSPI for IP Telephony installation. The password is stored in an encrypted format. You must be logged on as root/administrator to run this command.

## PARAMETERS

**encryptiptpasswd.ovpl -c ipt**

**encryptiptpasswd.ovpl -e ipt <new-password>**

-c ipt	This option helps you update the iSPI for IP Telephony jboss application server with the changed NNMi system account password.
-e ipt <new- password>	This option helps you modify the password of the Web Service Client user (used during the iSPI for IP Telephony installation).

## EXAMPLES

To update the iSPI for IP Telephony jboss application server with the changed NNMi system account password, run the following command:

```
$InstallDir/bin/encryptpasswd.ovpl -c ipt
```

To modify the password of the Web Service Client user, run the following command:

```
$InstallDir/bin/encryptpasswd.ovpl -e ipt password123
```

**password123** is the new password.

## AUTHOR

**encryptpasswd.ovpl** was developed by Hewlett-Packard Company.

## FILES

The **encryptpasswd.ovpl** uses the following files:

**\$NnmInstallDir/nonOV/ipt/jboss/server/nms/conf/props/nms-users.properties:** NNMi system account's credentials are stored in this file.

**\$NNM\_DATA//shared/ipt/conf/nnm.extended.properties:** This file stores the credentials of the Web Service Client user.

## Index

---

### C

Cisco Circuit Switched Channels	54
Cisco Circuit Switched Interfaces	53
Configuring	
Polling of Cisco CallManagers	15, 17, 19-21, 25-29, 31-35
Polling of Cisco gatekeepers	24
Control path	118

### E

encryptptpasswd.ovpl	121
----------------------	-----

### I

Incidents	99
iptjboss	120

### M

Monitoring	
Avaya IP phones	78
Cisco CallManagers	44
Cisco gatekeepers	50
Cisco IC trunks	49
Cisco IP phones	47
Cisco voice gateways	52
Nortel Call Servers	56
Nortel IP phones	59
Nortel QOS Zone view	62
Nortel Signaling Servers	58

### V

Views	42
Voice path	118

---