HP Network Node Manager iSPI for IP Telephony Software

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

Software Version: 9.21

Deployment Guide

Document Release Date: June 2013
Software Release Date: June 2013

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

Acknowledgements

This product includes software developed by Apache Software Foundation. (http://www.apache.org)

This product includes software developed by Indiana University Extreme! Lab.

This product includes software developed by SSHTools (http://www.sshtools.com/).

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

Oracle Technology — Notice of Restricted Rights

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

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

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

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

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

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

Support

Visit the HP Software Support Online web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

1 Introducing the NNM iSPI for IP Telephony

HP Network Node Manager i Software Smart Plug-in for IP Telephony (iSPI for IP Telephony) helps you extend the capability of HP Network Node Manager i Software (NNMi) to monitor the overall health of the network.

The factors that impact the deployment of the NNM iSPI for IP Telephony include the type of database configured with NNMi and the size of the network that you want to monitor. In addition, make sure to install the latest NNMi patches before installing the iSPI for IP Telephony.

Plan the deployment of the NNM iSPI for IP Telephony based on how NNMi is deployed in the environment. While planning the deployment, consider the following to achieve an optimum size and performance of the system:

- Number of managed IP telephony nodes
- Number of managed non-IP telephony nodes
- Deployment of the NNM iSPI for IP Telephony in a High Availability (HA) environment
- Deployment of the NNM iSPI for IP Telephony in an Application Failover environment
- Deployment of the NNM iSPI for IP Telephony in a Global Network Management (GNM) environment
- Deployment of the NNM iSPI for IP Telephony along with other iSPIs (iSPI for IP Multicast and iSPI for IP Telephony)

Preparing for Deployment

Before you start deploying the iSPI for IP Telephony, you must plan the installation based on your deployment requirements. You must identify the supported configurations, make sure that your installation process complies with all the prerequisites.

To install and configure the NNM iSPI for IP Telephony in a HA and Application failover environment, see the *HA and Application Failover* section of the *NNMi Deployment Reference Guide*.

Read the following NNMi documents before you start installing and configuring the iSPI for IP Telephony:

- *HP Network Node Manager i Software Deployment Reference*
- *HP Network Node Manager i Software Release Notes*
- *HP Network Node Manager i Software Support Matrix*

In addition, read the following NNM iSPI for IP Telephony documents before you start deploying the NNM iSPI for IP Telephony:

- *NNM iSPI for IP Telephony Installation Guide* 9.20

- *NNM iSPI for IP Telephony Release Notes* 9.20
- *NNM iSPI for IP Telephony Support Matrix* versions *9.20*

Make sure that you refer to the latest documents from **http://h20230.www2.hp.com/selfsolve/manuals**.

2 Deploy the NNM iSPI for IP Telephony

You must start deploying the NNM iSPI for IP Telephony after installing NNMi on a system. To install and configure NNMi on a system, see the *NNMi Installation Guide*.

You must install NNMi and the NNM iSPI for IP Telephony on the same server.

You can deploy the NNM iSPI for IP Telephony for the following scenarios:

- Install NNMi and the NNM iSPI for IP Telephony together.
- Install the NNM iSPI for IP Telephony on a system where NNMi is already installed.
- Install the iSPI for IP Telephony, NNMi, and the iSPI Performance for Metrics on the same system.
- Install the NNM iSPI for IP Telephony and NNMi on one system and the iSPI Performance for Metrics on a different system. You can choose this scenario for the best performance results.

See the *HP NNM i Software Smart Plug-in for IP Telephony Installation Guide* for more information about installing the iSPI for IP Telephony.

Deploying NNMi and the NNM iSPI for IP Telephony Together

To deploy the NNM iSPI for IP Telephony on a management server after installing NNMi, follow these steps:

1 Start the NNMi installation process.

You must use the database type (Embedded or Oracle) you used for the NNMi installation when you install the iSPI for IP Telephony.

2 Install the iSPI for IP Telephony. Follow the steps listed in the *HP NNM i Software Smart Plug-in for IP Telephony Installation Guide* to perform the steps during the pre-installation, installation, and the post installation phases.

Make sure that you have tuned the **`Xmx`** values in the `jboss properties` file of NNMi and iSPI for IP Telephony. To update the **`Xmx`** values, see the steps listed in *Tuning the jboss Memory* section of the *iSPI for IP Telephony, Support Matrix*.

Also, see the *iSPI for IP Telephony, Support Matrix* for recommended values as applicable for the size of your network.

3 Modify the values in `nms-ds.xml` and `postgresql.conf` as mentioned in Tuning Embedded Database for Scalability and Performance of NNMi and iSPI for IP Telephony on page 27.

4 Restart the NNMi and NNM iSPI for IP Telephony processes.

5 Configure the auto-discovery rules for IP phones. For more information, see the Setting NNMi Auto-Discovery Rules to Discover IP Phones on page 28.

6 Seed the IP telephony devices from the NNMi console. Seeding enables NNMi to start the discovery process and the NNM iSPI for IP Telephony nodes are discovered along with NNMi nodes. See the *HP NNM i Software Smart Plug-in for IP Telephony Installation Guide* for more information about seeding nodes for the iSPI for IP Telephony.

7 Wait for sometime till the NNM iSPI for IP Telephony nodes are discovered. Log on to the NNMi console, and then verify the availability of the IP Telephony workspace and IP Telephony views.

Deploying the NNM iSPI for IP Telephony where NNMi is Already Installed

To deploy the NNM iSPI for IP Telephony on a management server where NNMi is installed, follow these steps:

1 Install the NNM iSPI for IP Telephony on a management server where NNMi is already installed, running and the nodes are discovered. Follow the steps listed in the *HP NNM i Software Smart Plug-in for IP Telephony Installation Guide* to perform the steps during the pre-installation, installation, and the post installation phases.

➤ You must use the database type (Embedded or Oracle) you used for the NNMi installation when you install iSPI for IP Telephony.

➤ Follow the instructions in Step 3 only if you are using an embedded database. For the Oracle database, go to Step 4

2 Modify the values in `nms-ds.xml` and `postgresql.conf` as mentioned in Sizing and Configurations for Scalability and Performance of the iSPI for IP Telephony on page 27.

3 Restart the NNMi and NNM iSPI for IP Telephony processes.

4 Configure the auto-discovery rules for IP phones. For more information, see the Setting NNMi Auto-Discovery Rules to Discover IP Phones on page 28.

5 You can start the NNM iSPI for IP Telephony discovery process to discover the IP Telephony nodes from the discovered NNMi nodes in any *one* of the following ways:

- Run the configuration poll on each node (except on nodes that host IP phones) from NNMi Inventory workspace. For more information, see *Help for NNMi, Launch the Actions: Configuration Poll Command*.
- Wait for the next NNMi discovery cycle to rediscover the nodes and also start the discovery of the NNM iSPI for IP Telephony nodes.

Installing and Upgrading the NNM iSPI for IP Telephony in an HA Cluster

You can install NNMi and NNM iSPI for IP Telephony in a High Availability (HA) environment to achieve redundancy in your monitoring setup. The prerequisites to configure the NNM iSPI for IP Telephony in an HA environment is similar to NNMi. For information, see *NNMi Deployment Reference* guide.

Installing the NNM iSPI for IP Telephony

You can configure the NNM iSPI for IP Telephony for the following scenarios:

- Install NNMi and the NNM iSPI for IP Telephony in your environment before configuring NNMi to run under HA. See Configuring an HA Cluster on a Set of Systems with NNMi and iSPI on page 13.
- Install and configure the NNM iSPI for IP Telephony in an existing NNMi HA cluster environment. See Installing the NNM iSPI for IP Telephony in an Existing NNMi HA Cluster Environment on page 15.

If you configure the NNM iSPI for IP Telephony to use the PKI authentication when the NNM iSPI for IP Telephony is in HA cluster, you must perform all the required changes on both, primary (active) and secondary (passive) nodes. Before making the required changes for PKI authentication, make sure that NNMi and NNM iSPI for IP Telephony are running on one of the cluster members, and then move primary and secondary nodes to the maintenance mode. For information on required changes, see Configuring Access with Public Key Infrastructure Authentication on page 48.

Configuring an HA Cluster on a Set of Systems with NNMi and iSPI

If you have NNMi and the NNM iSPI for IP Telephony installed on at least two systems, you can create an HA cluster and configure NNMi and the iSPI to run under HA.

You can configure NNMi and NNM iSPI for IP Telephony on the primary node and secondary node in an HA environment. For more information on how to install NNMi in an HA environment, see *NNMi Deployment Reference*.

Configure the NNM iSPI for IP Telephony on the Primary Node

To configure the NNM iSPI for IP Telephony on the primary node, follow these steps:

1. Install NNMi and NNM iSPI for IP Telephony on each system. See the *NNMi Installation Guide* and the *NNM iSPI for IP Telephony Installation* guide for more information.
2. Configure the HA software on the systems and configure NNMi to run under HA. See the *NNMi Deployment Reference* for information on configuring NNMi to run under HA. Do not start the resource group while configuring NNMi to run under the HA (do not run the `nnmhastartrg.ovpl` command).
3. Configure the NNM iSPI for IP Telephony on the primary (active) node:
   a. Run the following command to find the virtual hostname:

nnmofficialfqdn.ovpl

b Modify the following files from the *$NnmdataDir*/`shared/ipt/conf` or *%NnmdataDir%*`\shared\ipt\conf` to replace the host name with the virtual FQDN for the following parameters:

File Name	Variable Name
`nms-ipt.jvm.properties`	`-Dcom.hp.ov.nms.ssl.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.spi.hostname`

c Modify the `server.properties` file from the `%nnmdatadir%\nmsas\ipt` or `/var/opt/OV/nmsas/ipt` directory to reflect the virtual FQDN of the NNMi management server for the `java.rmi.server.hostname` and `nmsas.server.net.hostname.private` parameters).

d Modify the `login-config.xml` file from the `%nnminstalldir%\ipt\server\conf` or `/opt/OV/ipt/server/conf` directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).

e Modify the relevant files in the following directories with the up-to-date information on both the primary and secondary cluster nodes:

For UNIX:

`/var/opt/OV/shared/ipt/conf`

For Windows:

`%NnmDataDir%\shared\ipt\conf`

f Run the following command to start the NNMi HA resource group:

— *For Windows:*

%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM <resource_group>

— *For UNIX*:

/opt/OV/misc/nnm/ha/nnmhastartrg.ovpl NNM <resource_group>

For more information, see *NNMi Deployment Reference* guide.

The NNM iSPI for IP Telephony and NNMi must start after this step. If NNMi or the NNM iSPI for IP Telephony does not start, see *Troubleshooting the HA Configuration* from *NNMi Deployment Reference*.

g Run the following command to configure the NNM iSPI for IP Telephony to run under the HA cluster:

— *For Windows:*

%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon IPT

— *For UNIX:*

/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon IPT

4 Configure the NNM iSPI for IP Telephony on the secondary (passive) node:

a Install NNMi with NNM iSPI for IP Telephony on the secondary node. Make sure the secondary node has a separate Fully Qualified Domain Names (FQDN) during the installation. See the *NNMi Installation Guide* and the *NNM iSPI for IP Telephony Installation* guide for more information.

a Run the following command to find the virtual hostname:

nnmofficialfqdn.ovpl

b Modify the following files from the *$NnmdataDir*/nmsas/ipt/conf or *%NnmdataDir%*\nmsas\ipt\conf to replace the host name with the virtual FQDN for the following parameters:

File Name	Variable Name
nms-ipt.jvm.properties	-Dcom.hp.ov.nms.ssl.keystore.alias
nnm.extended.properties	com.hp.ov.nms.spi.ipt.Nnm.hostname
nnm.extended.properties	com.hp.ov.nms.spi.ipt.spi.hostname

c Modify the server.properties file from the %nnmdatadir%\nmsas\ipt or /var/opt/OV/nmsas/ipt directory to reflect the virtual FQDN of the NNMi management server for the java.rmi.server.hostname and nmsas.server.net.hostname.private parameters).

d Modify the login-config.xml file from the %nnminstalldir%\ipt\server\conf or /opt/OV/ipt/server/conf directory to reflect the virtual FQDN of the NNMi management server (for the module-option element).

e Modify the relevant files in the following directories with the up-to-date information on both the primary and secondary cluster nodes:

For UNIX:

/var/opt/OV/shared/ipt/conf

For Windows:

%NnmDataDir%\shared\ipt\conf

f Run the following commands to configure the NNM iSPI for IP Telephony on the secondary node to run under the HA cluster:

— For Windows:

*%NnmInstallDir%***misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon IPT**

— For UNIX:

/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon IPT

5 Repeat step 4 on page 14 on each passive node in the HA cluster.

Installing the NNM iSPI for IP Telephony in an Existing NNMi HA Cluster Environment

You can configure the NNM iSPI for IP Telephony on the primary node and secondary node in an NNMi HA cluster environment. For more information on how to install NNMi in an HA environment, see *NNMi Deployment Reference* guide.

1 Make sure that NNMi is running on the primary server.

2 Put the NNMi resource group to the HA maintenance mode by placing the maintenance file under the following directory:

%nnmdatadir%\hacluster*<resource_group_name>*

$NnmDataDir/hacluster/*<resource_group_name>*

3 Run **ovstatus -c** to make sure that ovjboss is running.

4 Install the NNM iSPI for IP Telephony on the primary (active) node in the cluster, but do *not* start the iSPI.

5 Modify the following files from the *$NnmdataDir*/`nmsas/ipt/conf` or *%NnmdataDir%*`\nmsas\ipt\conf` to replace the host name with the virtual FQDN for the following parameters :

File Name	Variable Name
`nms-ipt.jvm.properties`	`-Dcom.hp.ov.nms.ssl.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.spi.hostname`

g Modify the `server.properties` file from the `%nnmdatadir%\nmsas\ipt` or `/var/opt/OV/nmsas/ipt` directory to reflect the virtual FQDN of the NNMi management server for the `java.rmi.server.hostname` and `nmsas.server.net.hostname.private` parameters).

h Modify the `login-config.xml` file from the `%nnminstalldir%\ipt\server\conf` or `/opt/OV/ipt/server/conf` directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).

i Modify the relevant files in the following directories with the up-to-date information on both the primary and secondary cluster nodes:

For UNIX:

`/var/opt/OV/shared/ipt/conf`

For Windows:

`%NnmDataDir%\shared\ipt\conf`

6 Remove the `maintenance` file that you added in step 2 on page 15.

7 Initiate a failover to a secondary (passive) node in the cluster where you want to install the NNM iSPI for IP Telephony. Make sure that NNMi fails over and runs on the secondary server successfully.

8 On this system, follow these steps:

a Put the NNMi resource group to the HA maintenance mode by placing the `maintenance` file under the following directory:

`%nnmdatadir%\hacluster\`*<resource_group_name>*

`$NnmDataDir/hacluster/`*<resource_group_name>*

b Run **`ovstatus -c`** to make sure that `ovjboss` is running.

c Install the NNM iSPI for IP Telephony on this server., but do *not* start the iSPI.

d Modify the following files from the `/var/opt/OV/shared/ipt/conf` or *%NnmdataDir%*`\shared\ipt\conf` to replace the host name with the virtual FQDN for the following parameters :

File Name	Variable Name
`nms-ipt.jvm.properties`	`-Dcom.hp.ov.nms.ssl.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.spi.hostname`

e Modify the `server.properties` file from the `%nnmdatadir%\nmsas\ipt` or `/var/opt/OV/nmsas/ipt` directory to reflect the virtual FQDN of the NNMi management server for the `java.rmi.server.hostname` and `nmsas.server.net.hostname.private` parameters).

f Modify the `login-config.xml` file from the `%nnminstalldir%\ipt\server\conf` or `/opt/OV/ipt/server/conf` directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).

g Modify the relevant files in the following directories with the up-to-date information on both the primary and secondary cluster nodes:

For UNIX:

`/var/opt/OV/shared/ipt/conf`

For Windows:

`%NnmDataDir%\shared\ipt\conf`

h Remove the `maintenance` file that you added in step a on page 16.

9 If you have multiple nodes in the cluster, fail over to another passive server, and then repeat step a on page 16 through step h on page 17.

10 Fail over to the server that was active when you started this procedure.

11 Run the following command on the active server first, and then on all passive servers:

— *For Windows:*

`%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon IPT`

— *For UNIX:*

`/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon IPT`

12 Verify that the NNM iSPI for IP Telephony is successfully registered by running the following command:

> Make sure NNMi and the NNM iSPI for IP Telephony processes are running before you run the following command.

- *On Windows:*

  `%nnminstalldir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS`

- *On UNIX/Linux:*

  `/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS`

Licensing

You require two licenses to run the NNM iSPI for IP Telephony in an HA cluster:

- One production license tied to the IP address of one of the physical cluster nodes
- One non-production license tied to the virtual IP address of the NNMi HA resource group

After obtaining these licenses for the NNM iSPI for IP Telephony, follow the procedure in the *Licensing NNMi in an HA Cluster* section in the *NNMi Deployment Reference*.

Upgrading the NNM iSPI for IP Telephony in an HA Cluster

Before You Upgrade

If you monitor the Cisco IP telephony environment, you must perform these additional steps to be able to use the CDR data collection feature:

1. Remove all extension packs for the Cisco IP Telephony from the NPS system:
   a. Log on to the NPS as administrator or root.
   b. Go to the following directory:

      On Windows

      <NPS_Install_Dir>`\NNMPerformanceSPI\bin`

      On Linux

      `/opt/OV/NNMPerformanceSPI/bin`

   c. Run the following commands:
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_BChannel_Activity`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_Calls_Terminations_Types`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_CDR_Collection`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_GW_Calls`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_IP_Trunk_Calls`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_VM_Information`**
2. Delete all extension packs for the Cisco IP telephony from the NNMi management server:
   a. Go to the following directory:
      - *On Windows:* `%nnmdatadir%\shared\perfSpi\datafiles\extension\final`
      - *On UNIX/Linux:* `/var/opt/OV/shared/perfSpi/datafiles/extension/final`
   b. Manually delete the following files:
      - `Cisco_IPT_BChannel_Activity.tar.gz.processed`
      - `Cisco_IPT_BChannel_Activity.tar.gz`
      - `Cisco_IPT_Calls_Terminations_Types.tar.gz.processed`
      - `Cisco_IPT_Calls_Terminations_Types.tar.gz`
      - `Cisco_IPT_CDR_Collection.tar.gz.processed`
      - `Cisco_IPT_CDR_Collection.tar.gz`
      - `Cisco_IPT_GW_Calls.tar.gz.processedCisco_IPT_GW_Calls.tar.gz`
      - `Cisco_IPT_IP_Trunk_Calls.tar.gz.processed`
      - `Cisco_IPT_IP_Trunk_Calls.tar.gz`
      - `Cisco_IPT_VM_Information.tar.gz.processed`

— `Cisco_IPT_VM_Information.tar.gz`

3 ○*Oracle database only.* Drop the following Oracle tables manually in the given order:

a ciscovmdevice

b vmdevice

c cktswitchedif

d monitoredcktswiface

e SIPSignalGateway

f SignalGateway

g CiscoGateKeeper

h Iptciscogatekeeperstatus

i NORTELH323GK

j H323Gatekeeper

4 *Oracle database only.* Drop the following Oracle tables manually (you need not follow the given order):

- ccmindex
- ciscocallmanagertogkmapper
- ciscounity
- h323trunkstate
- producttype
- routegrpnametodevnamemapping
- ciscocmexpress
- ciscocallmanager
- ciscocktswitchedchannel
- ciscocktswitchedifciscoextension
- ciscoh323gateway
- ciscomediagateway
- ciscosipgateway
- ciscosrstrouter
- ciscocallcontroller
- ciscovoicegateway
- cktswitchedchannel
- monitoredchannelinterface
- h323trunk
- mediasignalgateway
- CiscoRLRGMapping
- CiscoRGDeviceMapping
- CiscoUnityPolledAttributes

- channelstatusconclusion
- ciscoextensionstatusconclusion
- ciscovmstatusconclusion
- cktswitchedifstatusconclusion
- gkictstatusconclusion
- ciscoextensionstatus
- ciscovmstatus
- cktswitchedchannelstatus
- cktswitchedifstatus
- ciscogkcontrolledictstatus
- H323SignalGateway

5 Note down the CDR collection configuration details:

   a Go to the NNM iSPI for IP Telephony Configuration console.

   b Click **Data Access Configuration**. This opens the NNM iSPI for IP Telephony Data Access Configuration form. Click the **Cisco** tab, and then click the **CDR Access** tab.

   c Note down all the configuration details available in this form.

6 Create the following directory:

   Windows

   `<Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection`

   UNIX/Linux

   `/nnm_mount_point/NNM/dataDir/shared/ipt/IPTCiscoCDRCollection`

7 *On Windows.* Set the following directory as the home directory for the FTP server:

   `<Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection`

8 Create a user with read-write access to the following location:

   Windows

   `<Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection`

   UNIX/Linux

   `/nnm_mount_point/NNM/dataDir/shared/ipt/IPTCiscoCDRCollection`

9 *Only if you want to use the Billing Server mode.* Configure the Cisco Unified Communication Manager to export CDR files into the newly created directory (`<Shared_Drive>\NNM\dataDir\shared\ipt\IPTCiscoCDRCollection` or `/nnm_mount_point/NNM/dataDir/shared/ipt/IPTCiscoCDRCollection`) on the NNMi management server. This configuration task is performed in the Cisco Unified Serviceability console by specifying the Billing Application Server parameters.

10 Upgrade NNMi to the version 9.20.

11 Upgrade NPS to the version 9.20. Skip this step if you do not use the NNM iSPI for IP Telephony reports and do not have the NPS installed in your environment.

In this instance, `<Shared_Drive>` (Windows) or `/nnm_mount_point` (UNIX/Linux) is the directory location for mounting the NNMi shared disk.

Upgrade to the NNM iSPI for IP Telephony 9.20

To upgrade the NNM iSPI for IP Telephony to the version 9.20 in an HA cluster, follow these steps:

1. On the primary (active) NNMi management server in the cluster, follow these steps:
   a. Put the NNMi resource group to the HA maintenance mode by placing the `maintenance` file under the following directory:

      `%nnmdatadir%\hacluster\<resource_group_name>`

      `$NnmDataDir/hacluster/<resource_group_name>`

   b. Upgrade NNMi to the version 9.20. See the *NNMi Upgrade Reference* for more information.

   c. Run **`ovstatus -c`** to make sure that `ovjboss` is running.

   d. Upgrade the NNM iSPI for IP Telephony to the version 9.20.

   e. Stop the `ovjboss` process.

   f. Make sure that the following files from the `/var/opt/OV/nmsas/ipt/conf` or *%NnmdataDir%*`\nmsas\ipt\conf` contain the virtual FQDN for the following parameters :

File Name	Variable Name
`nms-ipt.jvm.properties`	`-Dcom.hp.ov.nms.ssl.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.spi.hostname`

   g. Make sure that the `server.properties` file from the `%nnmdatadir%\nmsas\ipt` or `/var/opt/OV/nmsas/ipt` directory contains the virtual FQDN of the NNMi management server for the `java.rmi.server.hostname` and `nmsas.server.net.hostname.private` parameters).

   h. Make sure that the `login-config.xml` file from the `%nnminstalldir%\ipt\server\conf` or `/opt/OV/ipt/server/conf` directory contains the virtual FQDN of the NNMi management server (for the `module-option` element).

   i. Modify the relevant files in the following directories with the up-to-date information on both the primary and secondary cluster nodes:

      For UNIX:

      `/var/opt/OV/shared/ipt/conf`

      For Windows:

      `%NnmDataDir%\shared\ipt\conf`

   j. Run the following command:

      `ovstart -c`

2. On the secondary (passive) node in the cluster, follow these steps:
   a. Put the NNMi resource group to the HA maintenance mode by placing the `maintenance` file under the following directory:

      `%nnmdatadir%\hacluster\<resource_group_name>`

`$NnmDataDir/hacluster/<resource_group_name>`

b Upgrade NNMi to the version 9.20, but do *not* start NNMi.

c Upgrade the NNM iSPI for IP Telephony to the version 9.20,

d Stop all NNMi and iSPI processes.

e Make sure that the following files from the `/var/opt/OV/nmsa/ipt/conf` or *%NnmdataDir%*`\nmsas\ipt\conf` contain the virtual FQDN for the following parameters :

File Name	Variable Name
`nms-ipt.jvm.properties`	`-Dcom.hp.ov.nms.ssl.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.spi.hostname`

f Make sure that the `server.properties` file from the `%nnmdatadir%\nmsas\ipt` or `/var/opt/OV/nmsas/ipt` directory contains the virtual FQDN of the NNMi management server for the `java.rmi.server.hostname` and `nmsas.server.net.hostname.private` parameters).

g Make sure that the `login-config.xml` file from the `%nnminstalldir%\ipt\server\conf` or `/opt/OV/ipt/server/conf` directory contains the virtual FQDN of the NNMi management server (for the `module-option` element).

h Modify the relevant files in the following directories with the up-to-date information on both the primary and secondary cluster nodes:

For UNIX:

`/var/opt/OV/shared/ipt/conf`

For Windows:

`%NnmDataDir%\shared\ipt\conf`

3 Repeat step 2 on page 21 on each passive node.

4 Make sure that the contents of the files present in the `/var/opt/OV/shared/ipt/avayacdr/conf` or `%nnmdatadir%shared\ipt\avayacdr\conf` directory are identical on the primary server as well as the secondary server.

5 Make sure that the contents of the files present in the `/var/opt/OV/shared/ipt/NortelCSMessageCodes/conf` or `%nnmdatadir%shared\ipt\NortelCSMessageCodes\conf` are identical on the primary system as well as the secondary system.

6 Remove the `maintenance` file from all passive nodes in the cluster.

7 On the active server, run the following command:

`ovstop -c`

8 On the active node, start the resource group by running the **`nnmhastartrg.ovpl`** command. After the resource group is on-line, remove the `maintenance` file.

9 After upgrade, configure the NNM iSPI for IP Telephony again for the CDR data collection by specifying the details that you noted down in step 5 on page 20.

Patching the NNM iSPI for IP Telephony Under HA

If you have already configured NNMi and the NNM iSPI for IP Telephony 9.20 to work in an HA cluster, you must follow this section to apply necessary patches (for both NNMi and the NNM iSPI for IP Telephony).

To apply patches for NNMi and NNM iSPI for IP Telephony, follow these steps:

1. Determine which node in the HA cluster is active:
   - *Windows:*

     **%NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl **

     -group <resource_group> -activeNode
   - *UNIX/Linux:*

     **/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl **

     -group <resource_group> -activeNode
2. On the active node, put the NNMi HA resource group into maintenance mode by creating the following files:
   - *Windows:*

     %NnmDataDir%\hacluster\<resource_group>\maintenance

     %NnmDataDir%\hacluster\<resource_group>\maint_NNM
   - *UNIX/Linux*:

     /var/opt/OV/hacluster/<resource_group>/maintenance

     /var/opt/OV/hacluster/<resource_group>/maint_NNM

     Include the **NORESTART** keyword in both these files.
3. On all passive nodes, put the NNMi HA resource group into maintenance mode by creating the following files:
   - *Windows:*

     %NnmDataDir%\hacluster\<resource_group>\maintenance

     %NnmDataDir%\hacluster\<resource_group>\maint_NNM
   - *UNIX/Linux*:

     /var/opt/OV/hacluster/<resource_group>/maintenance

     %NnmDataDir%\hacluster\<resource_group>\maint_NNM

     Include the **NORESTART** keyword in both these files.
4. On the active node, follow these steps:
   a. Stop NNMi:

      ovstop -c

   b. Back up the shared disk by performing a disk copy.

   c. *Optional*. Use the nnmbackup.ovpl command or another database command to back up all NNMi data. For example:

      nnmbackup.ovpl -type offline -scope all -target nnmi_backups

For more information about this command, see *NNMi Backup and Restore Tools* section in the *NNMi Deployment Reference*.

d Apply the appropriate NNMi and NNM iSPI patches to the system.

e Start NNMi:

```
ovstart -c
```

f Verify that NNMi started correctly:

```
ovstatus -c
```

All NNMi services should show the state **RUNNING**.

5 On each passive node, apply the appropriate patches to the system.

6 On all passive nodes, take the NNMi HA resource group out of maintenance mode by deleting the maintenance file from the nodes.

7 On the active node, take the NNMi HA resource group out of maintenance mode by deleting the maintenance file from that node.

Deploying the NNM iSPI for IP Telephony in an Application Failover Environment

This section provides instructions to deploy the NNM iSPI for IP Telephony in different scenarios in an application failover environment.

Application Failover with Oracle Configured as the Database

Scenario 1: In this scenario, consider that you want to install the NNM iSPI for IP Telephony with NNMi and then configure application failover over a LAN or a WAN:

1 Install NNMi in the primary server mode server 1 and install NNMi in the secondary server mode on server 2.

If you are installing Oracle as the database, NNMi provides you options to install NNMi in the primary and secondary server modes for deployment in an application failover or a high availability environment.

2 Start NNMi on server 1

3 Install the NNM iSPI for IP Telephony on server 1.

4 Install Oracle as the database by following the steps listed in the *NNM iSPI for IP Telephony Installation Guide*.

5 After the installation of the iSPI for IP Telephony, install the NNM iSPI for IP Telephony non production license on server 1.

6 Merge the keystores on one server and copy the keystores to both the primary and the secondary servers. See the *NNMi Deployment Reference* for instructions.

7 Stop NNMi on server 1.

8 Start NNMi on server 2.

9 Install the NNM iSPI for IP Telephony on server 2.

10 Configure NNM iSPI for IP Telephony on server 2 with the database instance, user name, and password configured on server 1

11 After the installation of the iSPI for IP Telephony, install the NNM iSPI for IP Telephony non production license on server 2.

12 Configure application failover server 1 and server 2 according to the instructions provided in the *NNMi Deployment Reference Guide*.

Scenario 2: In this scenario, consider that you want to install the NNM iSPI for IP Telephony after configuring NNMi in an application failover environment:

1 Remove the NNMi application failover configuration and restore the old keystore and truststore specific to each server (server 1 and server 2 as mentioned in the previous scenario). See the *NNMi Deployment Reference Guide* for instructions.

2 Follow the steps listed in the previous scenario to install the NNM iSPI for IP Telephony and configure application failover between server 1 and server 2.

You must not perform the steps to install NNMi.

Installing the NNM iSPI for IP Telephony in an Application Failover Environment with the Embedded Database

Scenario 1: In this scenario, consider that you want to install the NNM iSPI for IP Telephony and NNMi in an application failover mode:

1 Install the NNM iSPI for IP Telephony and NNMi on the primary server and the secondary server.

2 After the installation of the iSPI for IP Telephony, install the NNM iSPI for IP Telephony non production licenses on both the servers.

3 Follow instructions given in the *NNMi Deployment Reference Guide* to configure NNMi in application failover mode. After this, the NNM iSPI for IP Telephony automatically gets configured in the application failover mode.

Scenario 2: In this scenario, consider that you want to install the NNM iSPI for IP Telephony after configuring NNMi in the application failover mode:

1 Remove the NNMi application failover configuration and restore the old keystore and truststore specific to the primary server and the secondary server configured. See the *NNMi Deployment Reference Guide* for instructions.

2 Install the NNM iSPI for IP Telephony on both the primary and the secondary servers.

3 After the installation of the iSPI for IP Telephony, install the NNM iSPI for IP Telephony non production license on both the servers.

4 Follow instructions given in the *NNMi Deployment Reference Guide* to configure NNMi in application failover mode.

Guidelines for Discovery

- Discovering Cisco SRST routers by the NNM iSPI for IP Telephony:
  - Make sure that the Cisco SRST routers are already discovered by NNMi.

— Run the Configuration Poll action on Cisco Unified Communication Manager systems that belong to the cluster that hosts the Cisco SRST routers.

Cisco SRST routers are discovered after the next polling cycle is complete.

Deploying the NNM iSPI for IP Telephony in a Global Network Management Environment

You can deploy the NNM iSPI for IP Telephony in a Global Network Management (GNM) environment. The NNM iSPI for IP Telephony supports the following scenarios in a GNM environment. Consider the following points when you deploy the NNM iSPI for IP Telephony in a GNM environment:

- You can enable automatic discovery for a large group of nodes that host IP phones, up to 50,000, on the regional manager along with the seeding of the related neighboring switches and routers.
- You can create automatic discovery rules to discover the nodes (that host IP phones) across the regional managers and classify the nodes based on the clusters (for Cisco) and Communication Manager (for Avaya). You can then seed all the Cisco Call Managers and all the Avaya Communication Managers with the global manager. You can also seed all the nodes that host the Cisco Gatekeepers, Cisco Gateways, Cisco Unity devices, Cisco Call Manager Express, Cisco SRST, Avaya Communications Manager, Avaya LSP, and Avaya Media Gateways on the global manager.
- The NNM iSPI for IP Telephony can be run on the global manager only if the scalability limit for a single instance of the NNM iSPI for IP Telephony along with NNMi is within the supported limits. You must also make sure that the latency is minimal in the network path between NNMi and the managed nodes that host IP telephony entities across the WAN (possibly for geographic dispersed regions). See Performance and Scalability Metrics for the iSPI for IP Telephony for more information about the scalability limit.
- If the scalability limit is not high enough to exceed the limits supported with this version of the NNM iSPI for IP Telephony and if the latency is not a constraint, it is recommended to run the NNM iSPI for IP Telephony only on the global manager. You can make this decision when testing the latency aspect for SNMP across the WAN for nodes that host IP telephony entities.
- All the configuration changes done on the NNM iSPI for IP Telephony running on a regional manager are synchronized with the global manager during the subsequent polling cycle of the global manager.

See the *NNMi Deployment Reference Guide* for more information about GNM.

Scenario 1: NNMi and the NNM iSPI for IP Telephony on Global Manager and Regional Managers

In this scenario, all the regional managers send the IP Telephony information to the global manager. You can view the following information the global manager:

- Consolidated IP telephony topology
- Consolidated IP telephony reports

Scenario 2: NNMi and the NNM iSPI for IP Telephony on the Global Manager and NNMi on the Regional Managers

In this deployment scenario you can only see the locally managed IP telephony nodes by the global manager in the IP telephony inventory from the global manager.

Scenario 3: Deploying the Regional Manager in an Application failover Environment

When you deploy the NNM iSPI for IP Telephony regional manager in the Application failover environment, use the `ORDER` parameter to decide the priority to establish the connection with the regional manager from the global manager.

To use the regional manager in an application failover environment, follow these steps:

1. Configure the regional manager connection using the NNM iSPI for IP Telephony configuration workspace. See the *Adding a Regional Manager Configuration* section in the NNM iSPI for IP Telephony *Online Help* for more information.
2. Add two regional manager connections and provide the host names.
3. Use the `ORDER` parameter to give different values to the two regional managers.

Whenever an application failover occurs on the regional manager, the global manager establishes the next connection with the lowest order value. You can configure the regional manager in the application failover environment by following the steps documented in the Deploying the NNM iSPI for IP Telephony in an Application Failover Environment on page 24.

Sizing and Configurations for Scalability and Performance of the iSPI for IP Telephony

For sizing information of the iSPI for IP Telephony, see the *NNM iSPI for IP Telephony Support Matrix*.

To achieve optimal performance and scalability of NNMi and the iSPI for IP Telephony, see the following sections:

- Tuning Embedded Database for Scalability and Performance of NNMi and iSPI for IP Telephony on page 27
- Tuning NNMi Polling Configurations for Performance and Scalability of NNMi and NNM iSPI for IP Telephony on page 28.

Tuning Embedded Database for Scalability and Performance of NNMi and iSPI for IP Telephony

If you are using an embedded database while installing the iSPI for IP Telephony, update the following files:

Stop all the processes and make sure to take a backup of the files listed below.

- Modify the value default value=60 to 120 specified as `<max-pool-size>60</max-pool-size>` in the `nms-ds.xml` from

  `<INST_DIR>/nonOV/jboss/nms/server/nms/deploy/nms-ds.xml.`

  For example: If you have to change the default value=60 to 120, then change the `<max-pool-size>120</max-pool-size>.`

- Modify the value of `max_connections=100 to max_connections=200` from

  `<DATA_DIR>/shared/nnm/databases/Postgres/postgresql.conf`

After updating the above files, restart both the NNMi and NNM iSPI for IP Telephony processes.

Tuning NNMi Polling Configurations for Performance and Scalability of NNMi and NNM iSPI for IP Telephony

To increase the performance of NNMi with iSPI for IP Telephony, disable the polling for IP Phones, follow the steps:

1. From the **Monitoring Configuration** workspace, click **Node Settings** tab.
2. To view the details, click the **Open** icon with Ordering column specified as `400` which corresponds to Non-SNMP devices.
3. From the Fault Monitoring, clear the check boxes preceding `Enable ICMP Fault Polling`, `Enable SNMP Fault Polling`, and `Enable Component Health Fault Polling`.
4. To save the configuration, click **Save and Close.**

Setting NNMi Auto-Discovery Rules to Discover IP Phones

To set the Auto-discovery rules in NNMi to discover IP phones as non-SNMP devices, follow the steps:

1. From the **Discovery Configuration**, click **Auto-Discovery Rules** tab.

Make sure to check the left pane for the `Node Name Resolution` section. For first choice, select **IP Address**. Similarly, for second choice, select **Short sysName** and for third choice, select **Short DNS Name**.

2. From the **Auto-Discovery Rules** tab, add a new rule. From the left pane, **Basics** section, type the details such as Name and Ordering. For more information, see the *Help for NNMi*.

Make sure to select the check box for **Discover Non-SNMP Devices** and clear the check box for **Enable Ping Sweep**.

3. From the **IP Address Ranges for this Rule**, click **New** and add the range of IP addresses of call managers that manage IP phones in your IP telephony environment.
4. To save the configuration, click **Save and Close.**

If NNMi discovers and stores the details of the Cisco and Avaya IP phones, you may enable the custom attributes for the Cisco and Avaya IP phones. If you enable the custom attributes for the Cisco and Avaya IP phones, you can see the phone icons for all the discovered Cisco and Avaya IP phones in the NNMi topology maps.

To enable custom attributes for the Cisco IP phones:

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

To enable custom attributes for the Avaya IP phones:

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

3 Upgrading to the Version 9.20

You can upgrade the NNM iSPI for IP Telephony 9.10 (with the patch 2 or higher) to the version 9.20.

Before You Upgrade

If you monitor the Cisco IP telephony environment, you must perform these additional steps to be able to use the CDR data collection feature:

1. Note down the CDR collection configuration details:
   a. Go to the NNM iSPI for IP Telephony Configuration console.
   b. Click **Data Access Configuration**. This opens the NNM iSPI for IP Telephony Data Access Configuration form. Click the **Cisco** tab, and then click the **CDR Access** tab.
   c. Note down all the configuration details available in this form.
2. Create the following directory:

   Windows

   `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection`

   UNIX/Linux

   `/var/opt/OV/shared/ipt/IPTCiscoCDRCollection`
3. *On Windows.* Set the following directory as the home directory for the FTP server:

   `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection`
4. Create a user with read-write access to the following location:

   Windows

   `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection`

   UNIX/Linux

   `/var/opt/OV/shared/ipt/IPTCiscoCDRCollection`
5. *Only if you want to use the Billing Server mode.* Configure the Cisco Unified Communication Manager to export CDR files into the newly created directory (`%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection` or `/var/opt/OV/shared/ipt/IPTCiscoCDRCollection`) on the NNMi management server. This configuration task is performed in the Cisco Unified Serviceability console by specifying the Billing Application Server parameters.

Upgrading the NNM iSPI for IP Telephony

To upgrade the NNM iSPI for IP Telephony, follow these steps:

1. Uninstall all extension packs for the Cisco IP telephony from the NPS:

   Skip to step 2 if you do not use the NNM iSPI for IP Telephony reports and do not have the NPS installed in your environment.

   You must manually uninstall all Cisco IP telephony extension packs before upgrading to the NNM iSPI for IP Telephony 9.20. To uninstall all extension packs for the Cisco IP telephony, follow these steps:

   a. Log on to the NPS as administrator or root.

   b. Go to the following directory:

      On Windows

      <NPS_Install_Dir>`\NNMPerformanceSPI\bin`

      On Linux

      `/opt/OV/NNMPerformanceSPI/bin`

   c. Run the following commands:

      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_BChannel_Activity`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_Calls_Terminations_Types`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_CDR_Collection`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_GW_Calls`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_IP_Trunk_Calls`**
      - **`uninstallExtensionPack.ovpl -p Cisco_IPT_VM_Information`**

2. Make sure the NNM iSPI for IP Telephony 9.10 is installed on the management server with the latest patch.

3. Delete all extension packs for the Cisco IP telephony from the NNMi management server:

   Skip to step 4 if you do not use the NNM iSPI for IP Telephony reports and do not have the NPS installed in your environment.

   a. Go to the following directory:

      - *On Windows:* `%nnmdatadir%\shared\perfSpi\datafiles\extension\final`
      - *On UNIX/Linux:* `/var/opt/OV/shared/perfSpi/datafiles/extension/final`

   b. Manually delete the following files:

      - `Cisco_IPT_BChannel_Activity.tar.gz.processed`
      - `Cisco_IPT_BChannel_Activity.tar.gz`
      - `Cisco_IPT_Calls_Terminations_Types.tar.gz.processed`
      - `Cisco_IPT_Calls_Terminations_Types.tar.gz`
      - `Cisco_IPT_CDR_Collection.tar.gz.processed`

- — `Cisco_IPT_CDR_Collection.tar.gz`
- — `Cisco_IPT_GW_Calls.tar.gz.processed`
- — `Cisco_IPT_GW_Calls.tar.gz`
- — `Cisco_IPT_IP_Trunk_Calls.tar.gz.processed`
- — `Cisco_IPT_IP_Trunk_Calls.tar.gz`
- — `Cisco_IPT_VM_Information.tar.gz.processed`
- — `Cisco_IPT_VM_Information.tar.gz`

4 *Oracle database only.* Drop the following Oracle tables manually in the given order:

a ciscovmdevice

b vmdevice

c cktswitchedif

d monitoredcktswiface

e SIPSignalGateway

f SignalGateway

g CiscoGateKeeper

h Iptciscogatekeeperstatus

i NORTELH323GK

j H323Gatekeeper

5 *Oracle database only.* Drop the following Oracle tables manually (you need not follow the given order):

- ccmindex
- ciscocallmanagertogkmapper
- ciscounity
- h323trunkstate
- producttype
- routegrpnametodevnamemapping
- ciscocmexpress
- ciscocallmanager
- ciscocktswitchedchannel
- ciscocktswitchedif
- ciscoextension
- ciscoh323gateway
- ciscomediagateway
- ciscosipgateway
- ciscosrstrouter
- ciscocallcontroller
- ciscovoicegateway

- cktswitchedchannel
- monitoredchannelinterface
- h323trunk
- mediasignalgateway
- CiscoRLRGMapping
- CiscoRGDeviceMapping
- CiscoUnityPolledAttributes
- channelstatusconclusion
- ciscoextensionstatusconclusion
- ciscovmstatusconclusion
- cktswitchedifstatusconclusion
- gkictstatusconclusion
- ciscoextensionstatus
- ciscovmstatus
- cktswitchedchannelstatus
- cktswitchedifstatus
- ciscogkcontrolledictstatus
- H323SignalGateway

6 Upgrade NNMi to the version 9.20.

7 Upgrade NPS to the version 9.20. Skip this step if you do not use the NNM iSPI for IP Telephony reports and do not have the NPS installed in your environment.

8 Install the NNM iSPI for IP Telephony by following the instructions in the *NNM iSPI for IP Telephony 9.20 Installation Guide*.

9 After upgrade, configure the NNM iSPI for IP Telephony again for the CDR data collection by specifying the details that you noted down in step 1 on page 31.

Post-Upgrade Steps

The upgrade procedure does not retain the data that was collected by the previous version of the NNM iSPI for IP Telephony. It only retains the configuration data. Therefore, you must manually discover all IP telephony nodes (or wait for the next polling cycle) after upgrade. In addition, you must manually make tenant selections for a set of forms (because multi-tenancy was not supported for those forms with NNM iSPI for IP Telephony 9.10).

After upgrading to the NNM iSPI for IP Telephony 9.20, follow these steps:

If you use Mozilla Firefox, make sure to delete all cookies from the browser before you log on to the NNMi console.

1 Log on to the NNMi console as an administrator.

2 In the Workspaces navigation pane, click **Configure > NNM iSPI for IP Telephony Configuration**. The NNM iSPI for IP Telephony Configuration UI window opens.

3 Select a tenant of your choice for the following configuration forms:

By default, the `default` tenant is selected.

- Cisco AXL Data Access configuration
- Cisco phone inclusion filters
- Cisco phone exclusion filters
- Cisco QoS configuration
- Cisco CDR Data access configuration

4 Manually discover all IP telephony nodes.

Alternatively, use the iSPI inventories and reports only after the next polling cycle.

5 *Skip this step if you are not using the Oracle database.* Manually delete the following columns from the table, `extension`:

- `previouscallserver_id`
- `currentcallserver_id`

When you delete CUCM node from the NNMi inventory, the CUCM entity is not deleted from the NNM iSPI for IP Telephony inventory. You must delete these columns manually to make sure that CUCM entity is deleted from NNM iSPI for IP Telephony inventory also.

Licensing

The NNM iSPI for IP Telephony includes a temporary Instant-On license key that is valid for 60 days after you install the NNM iSPI for IP Telephony. You must obtain and install a permanent license key as soon as possible.The three types of the NNM iSPI for IP Telephony licenses are as follows:

- Instant-on: The Instant-on license is an evaluation license. The valid period of this license is sixty days with an unlimited capacity. The NNM iSPI for IP Telephony installs this license by default and you need not acquire this license from the HP License Key Delivery Service.
- iSPI Points Based: The iSPI Points-based licenses are common licenses for all the iSPIs that are used by all the Smart Plug-ins including the iSPI for IP Telephony.
- NNM iSPI for IP Telephony Migration Licenses: The migration licenses are valid only for the user updating from pervious versions (7x.x) of the iSPI for IP Telephony. Following are the valid migration licenses that you can obtain from HP License Key Delivery Service.

License Points Consumption Calculation

The raw consumption of license points by the NNM iSPI for IP Telephony is calculated as a sum of the IP telephony entities managed by the iSPI for IP Telephony. The points used in the 9.01 release of the product are as follows:

- 1 point for each IP Phone

- 3 points for each IP Telephony Gateway, for example, the Cisco Voice Gateway, the Avaya Media Gateway, or the Nortel Media Gateway
- 7 points for each Call Controller, for example, the Cisco Unified Communications Manager (Call Manager) or the Avaya Communication Manager or the Nortel Call Server.

For example if at any point of time there are 500 Cisco IP Phones, 1 Cisco Call Manager, and 1 Cisco Voice Gateway in your deployment environment, then the total raw consumption is calculated as follows: 1x7 + 1x3 + 500x1=510 points.

The various survivability options for the Call Controllers such as Cisco Survivable Remote Site Telephony (SRST) router or Avaya Local Survivable Processor (LSP) are not included while calculating the consumption of license points. The license points consumption calculation includes various light-weight options for call control such as Cisco Unified Communications Manager Express (CUCME) or Call Manager Express. The license points consumption calculation also includes the s8300-based standalone deployment of Avaya Communications Manager.

Points Licenses for New Installation for the NNM iSPI for IP Telephony

The points-based license system allows you to install a common pool of license points from where all the Smart Plug-ins can consume license points. The consumption from the common pool by the NNM iSPI for IP Telephony depends on the total raw consumption by the iSPI for IP Telephony. The NNM iSPI for IP Telephony consumes points from the common iSPI points license pool only when the consumption of the NNM iSPI for IP Telephony is more than the total capacity of the migration licenses installed.

This license system adds a base weight of 1000 points to any raw consumption of points from the common pool by the iSPI for IP Telephony. For example, if at any point of time there are 500 Cisco IP Phones, 1 Cisco Call Manager and 1 Cisco Voice Gateway in your deployment environment, then the common points consumption reported by NNM iSPI for IP Telephony is as follows: 1000 + 1x7 (one Call Manager) + 1x3 (one Gateway) + 500x1 (500 IP Phones)= 1510 points.

If the consumption of the license points is higher than the total license points in the common points pool or if other Smart Plug-ins consume from the common points pool that cause the total consumption of the points to exceed the available points in the common pool, the console displays a message to alert you. You can install additional Smart Plug-in license points to stop the display of the message.

You can acquire the license points from the HP License Key Delivery Service by entering your order number and selecting the appropriate Smart Plug-in points. The available license points are as follows:

- TA237AA HP NNM iSPI 100 Points Pack for 1-2500 Points SW LTU
- TA237AAE HP NNM iSPI 100 Points Pack for 1-2500 Points SW E-LTU
- TA238AA HP NNM iSPI 100 Points Pack for 2501-5000 Points SW LTU
- TA238AAE HP NNM iSPI 100 Points Pack for 2501-5000 Points SW E-LTU
- TA239AA HP NNM iSPI 100 Points Pack for 5001-10,000 Points SW LTU
- TA239AAE HP NNM iSPI 100 Points Pack for 5001-10,000 Points SW E-LTU
- TA240AA HP NNM iSPI 100 Points Pack for 10,001-25,000 Points SW LTU
- TA240AAE HP NNM iSPI 100 Points Pack for 10,001-25,000 Points SW E-LTU
- TA241AA HP NNM iSPI 100 Points Pack for 25,001-50,000 Points SW LTU

- TA241AAE HP NNM iSPI 100 Points Pack for 25,001-50,000 Points SW E-LTU
- TA242AA HP NNM iSPI 100 Points Pack for 50,000+ Points SW LTU
- TA242AAE HP NNM iSPI 100 Points Pack for 50,000+ Points SW E-LTU
- TA248AA HP NNM iSPI 100 Points Pack for 1-2500 Points Non-production SW LTU
- TA248AAE HP NNM iSPI 100 Points Pack for 1-2500 Points Non-production SW E-LTU
- TA249AA HP NNM iSPI 100 Points Pack for 2501-5000 Points Non-production SW LTU
- TA249AAE HP NNM iSPI 100 Points Pack for 2501-5000 Points Non-production SW E-LTU
- TA250AA HP NNM iSPI 100 Points Pack for 5001-10,000 Points Non-production SW LTU
- TA250AAE HP NNM iSPI 100 Points Pack for 5001-10,000 Points Non-production SW E-LTU
- TA251AA HP NNM iSPI 100 Points Pack for 10,001-25,000 Points Non-production SW LTU
- TA251AAE HP NNM iSPI 100 Points Pack for 10,001-25,000 Points Non-production SW E-LTU
- TA252AA HP NNM iSPI 100 Points Pack for 25,001-50,000 Points Non-production SW LTU
- TA252AAE HP NNM iSPI 100 Points Pack for 25,001-50,000 Points Non-production SW E-LTU
- TA253AA HP NNM iSPI 100 Points Pack for 50,000+ Points Non-production SW LTU
- TA253AAE HP NNM iSPI 100 Points Pack for 50,000+ Points Non-production SW E-LTU

Licensing for Upgrading (Migrating) from Earlier Versions

If you are upgrading from the 7.5x version of the iSPI for IP Telephony, then you can obtain the NNM iSPI for IP Telephony upgrade (migration) licenses. You can contact HP sales to know your upgrade license entitlement based on your order number for the 7.5x version of the iSPI for IP Telephony. For the iSPI for IP Telephony, the upgrade licenses are not unlimited and are based on the specific upgrades you select for license generation. You can select from the following NNM iSPI for IP Telephony upgrade licenses:

- TA245AA HP NNM iSPI for IP Telephony 250 Phones Pack Migration SW LTU
- TA245AAE HP NNM iSPI for IP Telephony 250 Phones Pack Migration SW E-LTU
- TA246AA HP NNM iSPI for IP Telephony 1000 Phones Pack Migration SW LTU
- TA246AAE HP NNM iSPI for IP Telephony 1000 Phones Pack Migration SW E-LTU
- TA247AA HP NNM iSPI for IP Telephony 5000 Phones Pack Migration SW LTU
- TA247AAE HP NNM iSPI for IP Telephony 5000 Phones Pack Migration SW E-LTU
- TA256AA HP NNM iSPI for IP Telephony 250 Phones Pack Migration Non-production SW LTU
- TA256AAE HP NNM iSPI for IP Telephony 250 Phones Pack Migration Non-production SW E-LTU
- TA257AA HP NNM iSPI for IP Telephony 1000 Phones Pack Migration Non-production SW LTU

- TA257AAE HP NNM iSPI for IP Telephony 1000 Phones Pack Migration Non-production SW E-LTU
- TA258AA HP NNM iSPI for IP Telephony 5000 Phones Pack Migration Non-production SW LTU
- TA258AAE HP NNM iSPI for IP Telephony 5000 Phones Pack Migration Non-production SW E-LTU

The points for the different licenses are as follows:

- 250 Phones Pack Migration licenses: 1500 points
- 1000 Phones Pack Migration licenses: 3000 points
- 5000 Phones Pack Migration licenses: 11000 points

If you install one or more valid upgrade licenses on the system, then the total capacity of the upgrade license points is a sum of the points for all the individual license keys installed. The NNM iSPI for IP Telephony does not consume license points from the common license points pool if the raw consumption of license points by the NNM iSPI for IP Telephony is less than or equal to the total upgrade license points installed. If the raw consumption exceeds the total capacity of upgrade licenses, the NNM iSPI for IP Telephony starts consuming license points from the common license points pool. The consumption from common points pool is calculated as 1000 + (total raw consumption-total migration capacity). For example, let us consider a case where you plan to upgrade and then install two TA247AA HP NNM NNM iSPI for IP Telephony 5000 Phones Pack Migration SW LTU licenses. The total upgrade capacity based on points is 11000x2 = 22000 points. Now consider the scenario, where on day 1 you have 21934 Cisco IP Phones, 5 Cisco Call Managers and 10 Cisco Voice Gateways. This makes the total raw consumption on day 1 as 5x7+ 3x10 + 21934x1 = 21999. This value being less then 22000, prevents the message on the console to alert you regarding the excessive point consumption.

Now consider the scenario when on day 2, the number of Cisco IP Phones increases to 22000 thus taking the total consumption to 22065. In this scenario, if there are no Smart Plug-in points licenses installed on the system, the consumption reported by the NNM iSPI for IP Telephony will be 22065 and this prompts a message on the console alerting you about the excess points consumed by the iSPI for IP Telephony. You must install some iSPI points licenses at this stage to get rid of the message. If you install 20 TA237AA HP NNM iSPI 100 Points Pack for 1-2500 Points SW LTU licenses, the total upgrade capacity increases by 2000 points. At this stage, the alert message from the console disappears and the consumption of Smart Plug-in license points by the NNM iSPI for IP Telephony is as follows: 1000 + (22065-22000) = 1065 points.

However, if the consumption increases further or if other Smart Plug-ins consume from the common points pool and the total consumption from the common points pool exceeds 2000, the console displays the alert message again and you must install additional Smart Plug-in points licenses to stop getting the alert messages on the console.

Note that on day 2, as an alternative, you can install additional NNM iSPI for IP Telephony upgrade licenses if you are entitled to obtain the required number of upgrade licenses from HP License Key Delivery Service. This stops the alert message from appearing on the console without you having to install additional common pool points licenses.

Viewing the Types of Licenses Installed and the Capacity

You can view the license information by selecting the following option from the NNMi console: **Help** > **System Information** > **View Licensing Information**

Installing Licenses

See the section *License Information* in the *NNM iSPI for IP Telephony Installation Guide* for instructions to install the different types of licenses.

4 Deploying in a Multiple Tenant Model

Multiple Tenant Model—An Overview

The multiple tenant model supported by NNMi helps you to logically group nodes in the NNMi database and assign security and user level permissions to these node groups. This helps in restricting the information about these nodes from being viewed by operators who are not designated to monitor these nodes. By default, all the operators have access to view all the nodes in the NNMi console. By assigning security and user level permissions to these node groups, you gain the following benefits:

- Restrict access to nodes in the NNMi database for operators who are not assigned for monitoring those nodes
- Customize operator views based on the nodes that the operator must monitor
- Simplify configuration of nodes and node groups
- Display the topology inventory based on the node access permissions for the operator
- Display the maps and path views relevant to the nodes that the operator is designated to monitor
- Perform actions using the NNMi console only on the nodes that are accessible to the operator
- Display incidents based on the nodes that the operator monitors

See the *NNMi Deployment Reference Guide* for more information about the multiple tenant model supported by NNMi.

Multiple Tenant Model for Cisco IP Telephony

For an enterprise with Cisco IP telephony infrastructure monitored using NNMi and the iSPI for IP Telephony, you must make sure that you follow the guidelines in this section to implement the multiple tenant model.

Call Managers

Make sure that you seed all the nodes hosting Cisco call managers in a cluster with the same tenant—security group combination. Failure to follow this guideline might result in inconsistent implementation of security and user level permissions for nodes.

IP Phones

The IP phones configured in any Cisco Unified Communications Manager (CUCM) in a Cisco Unified Communications Manager cluster derive the security groups based on the security group configured for the CUCM in the cluster. This indicates that an operator who has access to the CUCM in the cluster also has access to the IP phones configured with the CUCM.

Hosting Nodes for Gateways, Gatekeepers, Unity Devices, and SRST Routers

You can seed the nodes that host the gateways, gatekeepers, unity devices, and SRST routers using any security group—tenant combination. It is recommended to use the same security group—tenant combination configured for the CUCM in the cluster with which these devices are associated. Note that the iSPI for IP Telephony considers a gateway as a call routing device associated with a cluster. For the SRST router deployed for failover, you must make sure that you configure the same security group—tenant combination configured for the CUCM that is designated as the primary call controller.

Intercluster IP Trunks

The intercluster IP trunks derive the security group—tenant combination from the CUCM associated with the IP trunk. Note that the iSPI or IP Telephony considers the intercluster IP trunk as a call routing resource associated with a CUCM in the cluster.

Reporting

The metrics in the following extension packs for reporting derive the security group—tenant combination configured for the CUCM cluster that handles the call. This makes sure that the row level security in NPS is implemented along with multitenancy:

- Call Details
- Gateway Calls
- IP Trunk Calls
- Call Types and Termination Reasons

The Cisco BChannel Activity extension pack for reporting derives the security group—tenant combination from the Cisco Unity device or the Unity connection for which the metrics are applicable.

Multiple Tenant Model for Avaya IP Telephony

For an enterprise with Avaya IP telephony infrastructure monitored using NNMi and the iSPI for IP Telephony, you must make sure that you follow the guidelines in this section to implement the multiple tenant model.

Communication Managers

Make sure that both the nodes hosting the primary communication managers in a duplex redundant pair are seeded with the same security group—tenant combination. Failure to follow this guideline might result in inconsistent implementation of security and user level permissions for nodes.

IP Phones

The IP phones configured on any communication manager in a duplex redundant pair of primary communication manager or a standalone primary communication manager derive the security group—tenant combination from the nodes hosting any communication manager in the redundant pair or the node hosting the primary standalone communication manager. This indicates that an operator who has access to the communication manager in the redundant pair also has access to the IP phones configured with the communication manager.

Primary Communication Manager Servers, Local Survivable Processors, and H.248 Media Gateways

you can seed standalone primary communication manager servers, Local Survivable Processors (LSP) and H.248 media gateways using any security group—tenant combination. It is recommended that you seed the nodes hosting the H.248 media gateways with the same security group—tenant combination configured for the node hosting the primary communication manager (in the pair or in the standalone mode) that uses the H.248 media gateway for call routing.

For nodes hosting LSPs, it is recommended that you seed the nodes with the same security group—tenant combination configured for the node hosting the primary communication manager (in the pair or in the standalone mode) that acts as the primary call controller for the branch where the LSP is deployed for failover.

Port Network Media Gateways

The port network media gateways such as the G650 and the associated components supported by the iSPI for IP Telephony such as CLAN, IPSI, media processor, and so on derive the security group—tenant combination from the node hosting the primary communication manager (in the pair or in the standalone mode) to which the Port Network media gateway is associated.

Reporting

The metrics in the following extension packs derive the security group—tenant combination from the primary communication manager that handles the call. This makes sure that the row level security in NPS is implemented along with multitenancy:

- Call Details
- Gateway Calls
- Trunk Calls
- Call Types and Termination Reasons

The metrics in the following extension packs for reporting derive the security group—tenant combination from the primary communications manager that uses the trunk groups, route patterns, network regions, or port networks for which the metrics are applicable:

- Trunk Activity
- Trunk Group and Route Pattern Usage
- Processor Occupancy Summary
- Port Network Load Statistics
- Network Region DSP/CODEC Usage Summary

The metrics for the RTP Session Metrics extension pack derives the security group—tenant combination from the primary communications manager configured for the RTP endpoint.

Multiple Tenant Model for Microsoft IP Telephony

For an enterprise with Microsoft IP telephony infrastructure monitored using NNMi and the iSPI for IP Telephony, you must make sure that you follow the guidelines in this section to implement the multiple tenant model.

As an administrator, you must configure at least one front end pool for a central site, using the Add FrontEnd Pool Configuration page provided by the iSPI for IP Telephony. The iSPI for IP telephony uses this configuration information to retrieve information related to the topology, policies, CDR and QoE collection, and users from the central site. The iSPI for IP Telephony discovers the topology of the central site and all the associated branch sites through the seeded front end pool. The iSPI for IP Telephony also maps the tenant name (provided while configuring the front end pool), the tenant UUID, and the UUID of the default security group of the tenant with the front end pool.

During discovery, the iSPI for IP Telephony seeds the servers and gateways with NNMi and maps these entities with the tenant details associated with the front end pool. The iSPI for IP Telephony uses the tenant mapping for any entities discovered through the front end pool.

As voice policies, voice routes, dial plans, and normalization rule configuration settings can be associated to multiple frontend pools in an organization, the iSPI for IP Telephony groups these entities based on the tenants associated with the front end pools associated with these entities.

After NNMi completes the discovery of the servers and gateways, the iSPI for IP Telephony retrieves the security group information for the discovered entities and maps the security group information against the discovered entities. See the following points before deploying the iSPI for IP Telephony to monitor the Microsoft IP Telephony entities:

- You can access a Gateway or server if you are assigned to the same security group assigned to the corresponding NNMi node.
- You can access a site if you have access to at least one server in the site.
- You can access a SIP trunk configuration if you have access to the site that includes the SIP trunk.
- You can access all the Lync users of an organization if you are assigned to the default security group of the tenant with which the frontend pool was seeded.
- You can access all the policies of an organization if you are assigned to the default security group of the Tenant with which the frontend pool was seeded.
- You can access an end user group if you have access to at least one user in the end user group.
- A non-administrative user does not have access to the NNMi sites configured in the iSPI for IP Telephony.

5 Overlapping IP Addresses

If your network supports Network Address Translation (NAT) protocol or Port Address Translation (PAT) protocol, you must follow the instructions provided in the *Managing Overlapping IP Addresses in NAT Environments* section in the *NNMi Deployment Reference*.

In addition to the common instructions mentioned in the *NNMi Deployment Reference*, you must follow a few additional guidelines to monitor the IP telephony infrastructure.

Cisco IP Telephony

If you manage a Cisco IP telephony infrastructure in your enterprise, make sure that you follow these guidelines:

- All Cisco IP Telephony entities, such as Cisco Unified Communication Manager clusters, Cisco Unified Communication Manager Subscriber groups, Cisco Unified Communication Managers, gateways, Survivable Remote Site Telephony (SRST) routers, intercluster trunks, Unified Communication Manager Expresses, IP phones, gatekeepers, unity devices, and so on, that belong to an overlapping address domain must be associated with a single tenant.
- The NNM iSPI for IP Telephony discovers the Cisco IP phones using the internal (private) IP addresses of the IP phones. Therefore, you must map the external IP address and the internal IP address of all Cisco IP phones using Overlapping Address Mapping form of NNMi. If you do not complete this mapping, the NNM iSPI for IP Telephony may not be able to draw the voice paths and control paths correctly. For more information, see *NNMi Online Help, Overlapping IP Address Mapping*.
- When you configure the NNM iSPI for IP Telephony to access data with AXL and SSH, you must provide the external IP address (public address) of the Cisco Unified Communication Manager.

Avaya IP Telephony

If you manage an Avaya IP telephony infrastructure in your enterprise, make sure that you follow these guidelines:

- All Avaya IP Telephony entities, such as call controllers, IP phones, media gateways, and so on, that belong to an overlapping address domain must be associated with a single tenant.
- You must also map the external IP address and the internal IP address of all Avaya Media Processors and Avaya IP Server Interfaces (IPSIs) using the Overlapping Address Mapping form of NNMi.If you do not complete the mapping for these entities, the NNM iSPI for IP Telephony may not generate incidents related to these entities.
- The NNM iSPI for IP Telephony discovers the Avaya Control Local Area Networks (CLANs) and Avaya IP phones firstly using their internal (private) IP addresses. The NNM iSPI for IP Telephony seeds them to NNMi database later. You must map the external IP address and the internal IP address of all Avaya CLANs and Avaya IP phones

using Overlapping Address Mapping form of NNMi. If you do not complete this mapping, the NNM iSPI for IP Telephony may not be able to draw the voice paths and control paths correctly. The CLAN and IP phones association polling also may not take place. For more information, see *NNMi Online Help, Overlapping IP Address Mapping*.

- When you configure CDR Access, RTCP reception, and SSH access, you must provide the external IP address (public address) of the Avaya Communication Manager.

Overlapping Address Domain Support for Microsoft IP Telephony

If you manage a Microsoft IP telephony infrastructure in your enterprise, you must make sure that all Microsoft servers and gateways that belong to an overlapping address domain are associated with a single tenant.

6 Administration Tasks

This chapter provides you information on the administration tasks that you can perform after you have installed the iSPI for IP Telephony.

Enabling Single Sign On

See the section *Using Single Sign-on with NNMi* in the *HP Network Node Manager i Software Deployment Reference Guide* for an overview about single sign-on. You can perform this step to grant Single Sign-on (SSO) access to users who do not have the *system* privileges to access the NNMi console. SSO is not enabled during installation or when you upgrade from the previous versions.

You can enable SSO to allow the non system users to access the NNMi console, the configuration screens, and the integrated application screens by signing in once to the NNMi console.

You can enable single sign-on for the NNM iSPI for IP Telephony by following the steps listed:

For Windows

1. Edit the *%NnmDataDir%*`\shared\nnm\conf\props\nms-ui.properties` file. Change **`com.hp.nms.ui.sso.isEnabled= "false"`** to **`com.hp.nms.ui.sso.isEnabled = "true".`**
2. Run the **`nnmsso.ovpl -reload`** script.
3. Run the **`iptssoreload.ovpl`** script.

For UNIX

1. Edit the *$NnmDataDir*`/shared/nnm/conf/props/nms-ui.properties` file. Change **`com.hp.nms.ui.sso.isEnabled= "false"`** to **`com.hp.nms.ui.sso.isEnabled = "true".`**
2. Run the **`nnmsso.ovpl -reload`** script.
3. Run the **`iptssoreload.ovpl`** script.

Do not enable the Single Sign-On feature when NNMi and the NNM iSPI for IP Telephony are configured to use the Public Key Infrastructure (PKI) authentication.

Configuring Access with Public Key Infrastructure Authentication

You can configure NNMi to map Public Key Infrastructure (PKI) certificates to NNMi user accounts. As a result, you can log on to the NNMi console without having to type in the NNMi user name and password on the Login page. However, you will be prompted to provide NNMi user name and password again when you try to launch the NNM iSPI for IP Telephony forms, unless you perform additional steps to reconcile the mapping with the iSPI.

When NNMi is configured to use the PKI authentication, it is mandatory for the iSPI to use the PKI authentication. You must not configure only the iSPI to use the PKI authentication when NNMi continues to use the credentials-based authentication.

Configuring the iSPI to use the PKI authentication involves the following tasks:

- Configuring NNMi on page 48
- Configuring a Certificate Validation Method on page 48
- Configuring the NNM iSPI for IP Telephony on page 49

If you configure the NNM iSPI for IP Telephony to use the PKI authentication when the NNM iSPI for IP Telephony is in HA cluster, you must perform the required configuration tasks on both, primary (active) and secondary (passive) nodes.

Task 1: Configuring NNMi

To configure NNMi to use the PKI authentication, follow the steps in the *Configuring NNMi to Support Public Key Infrastructure Authentication* section in the *HP Network Node Manager Deployment Reference*.

After configuring NNMi to use the PKI authentication, if you do not perform Task 4 on page 49, you will be prompted to provide NNMi user name and password when you try to launch the NNM iSPI for IP Telephony forms.

Task 2: Configuring a Certificate Validation Method

When NNMi is configured to use the PKI authentication, unauthorized access using invalid certificates must be prevented. You must perform additional steps to configure NNMi to use a certificate validation method—Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP).

Follow the steps in the *Certificate Validation (CRL and OCSP)* section in the *HP Network Node Manager Deployment Reference*.

Task 3: Enabling SSL

When NNMi is configured to use the PKI authentication, you must enable SSL on the NNM iSPI for IP Telephony to ensure communication between the NNMi management server and the NNM iSPI for IP Telephony server.

To enable SSL on the NNM iSPI for IP Telephony, follow these steps:

1. Log on to the NNM iSPI for IP Telephony server.
2. Navigate to the following directory:

   On Windows

   ```
   %nnmdatadir%\shared\ipt\conf
   ```

   On Linux

/var/opt/OV/shared/ipt/conf

3 Open the nnm.extended.properties file with a text editor.

4 Set the value of following properties to true:

— com.hp.ov.nms.spi.ipt.spi.isSecure

— com.hp.ov.nms.spi.ipt.Nnm.isSecure

5 Save and close the file.

6 Restart the iptjboss process by running the following commands:

a **ovstop -c iptjboss**

b **ovstart -c iptjboss**

Task 4: Configuring the NNM iSPI for IP Telephony

Configuring NNMi to use the PKI authentication essentially requires updating the nms-auth-config.xml file, which is available in NNMi's configuration data directory (%nnmdatadir%\nmsas\NNM\conf on Windows; /var/opt/OV/nmsas/NNM/conf on UNIX/Linux). You must modify the nms-auth-config.xml file in the iSPI configuration data directory based on the updated nms-auth-config.xml file to enable the iSPI to use the PKI authentication.

To configure the NNM iSPI for IP Telephony to use the PKI authentication, follow these steps:

1 Make sure that Task 1, Task 2, and Task 3 are complete.

2 Log on to the NNMi management server.

3 Navigate to the following directory:

On Windows

%nnmdatadir%\nmsas\ipt\conf

On Linux

/var/opt/OV/nmsas/ipt/conf

4 Open the nms-auth-config.xml file with a text editor.

5 Modify the nms-auth-config.xml file on the iSPI to enable PKI authentication. For information on the required changes, see the Configuring NNMi for PKI (X.509 Certificate Authentication) section in the *HP Network Node Manager Deployment Reference*.

> Make sure that you modify the iSPI nms-auth-config.xml file to match the changes done to the nms-auth-config.xml file on the NNMi management server.

6 Save and close the file.

7 Run the following command at the command prompt:

On Windows

%nnminstalldir%\bin\nmsiptauthconfigreload.ovpl

On UNIX/Linux

/opt/OV/bin/nmsiptauthconfigreload.ovpl

Running the nmsiptconfigimport.ovpl Command

The `nmsiptconfigimport.ovpl` command requires you to provide NNMi's administrator user credentials as command-line arguments. When the iSPI is configured to use the PKI authentication, you can run the `nmsiptconfigimport.ovpl` command without providing any user credentials (that is, you can run the command without the `-u` and `-p` options).

However, make sure that the user account with which you logged on to the NNMi management server to run the command has READ access to the following file:

- *On Windows*

  `%nnmdatadir%\nmsas\ipt\conf\props\nms-users.properties`

- *On UNIX/Linux*

  `/var/opt/OV/nmsas/ipt/conf/props/nms-users.properties`

Adding IP Telephony Nodes after Installing the iSPI for IP Telephony

If you want to add more IP Telephony nodes (for example, CallManagers, Voice Gateways, Gatekeepers, and so on) to your deployment environment after installing the iSPI for IP Telephony, you must do as follows:

1. Use the iSPI for IP Telephony configuration workspace to specify the required settings for the newly added entities. See the *iSPI for IP Telephony Online Help* > **Help for Administrators** for more information.
2. Seed the nodes that host the IP Telephony entities using the *Discovery Configuration* form in the NNMi configuration workspace. See the *NNMi Online Help* for more information about seeding nodes.
3. Wait for the next discovery cycle by NNMi to trigger the discovery of the newly added IP Telephony entities. Alternatively, you can select the nodes from the NNMi node inventory and perform a configuration poll for the nodes. See the *NNMi Online Help* for more information about discovery cycles and performing configuration polls.

Recommendations for Configuring Data Access

You can use the following recommendations when configuring data access for both Cisco and Avaya using the *iSPI for IP Telephony Configuration* form.

Cisco Data Access Recommendations

You must provide the following details to configure data access for Cisco IP Telephony:

AXL Access Configuration Parameters:

Specify the following parameters to configure AVVID XML Layer (AXL) API exposed data:

- 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.

CDR Access Configuration Parameters:

You must make sure that the system time for the iSPI for IP Telephony server must be equal to or slower than the system time of the CDR repository server if both the servers belong to the same time zone. If the servers are in different time zones, the iSPI for IP Telephony uses the system time of the iSPI for IP Telephony server for CDR retrieval. This might cause the time stamp of the call data to be different when compared to the actual time of the call.

Before configuring CDR access, you must also make sure that the `CDRonDemand` Web Service is running on the Call Manager repository server.

You must provide the following details to configure CDR access:

- 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.

Make sure that you do not include blank space characters before or after the values you type.

You must also make sure that you have configured an FTP user name and password on the iSPI for IP Telephony server which the `CDRonDemand` Web Service uses to send CDR files to the iSPI for IP Telephony server. If you are running the iSPI for IP telephony on Microsoft Windows operating system, you must configure an FTP client and make sure that the `NnmDataDir\log\ipt\tmp` folder is shared for FTP user access.

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 `%NnmDataDir%\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.

Data Access Recommendations for Clusters

Make sure that you configure the iSPI for IP Telephony to access CDR data from all the clusters. You must note down the following details or each Cisco Call Manager Cluster in the environment and provide this information in the Data Access Configuration form for the iSPI for IP Telephony:

- The iSPI for IP Telephony supports collection of CDR data using both the Cisco supported mechanisms:

— Mechanism that requires the iSPI for IP Telephony to act as a billing server.

— mechanism that requires iSPI for IP Telephony to act as a web services client for the CDR-on-Demand Web Service hosted on a server node inside the cluster.

You must determine the mode used by a specific cluster before proceeding with CDR data access configuration.

— The billing server based collection requires you to do the required configuration on the call manager server in cluster that hosts the CDR repository node role for the cluster. The configuration includes specifying the following details:

— The fully qualified domain name of the iSPI for IP Telephony server as the designated billing server

— The FTP user name

— The FTP password

— The directory in the iSPI for IP Telephony server file-system where you want the CDR files to be uploaded by the CDR repository node in the cluster. Note that this directory usually is located at a relative path to the `$NnmDataDir/log/ipt/tmp` directory on the iSPI for IP Telephony server. The iSPI for IP Telephony requires you to set up the FTP server on the iSPI for IP Telephony in such a way that the home directory of the FTP user is a valid sub directory under the `$NnmDataDir/log/ipt/tmp` directory. Make sure that the CDR repository hosting node in the cluster has adequate ability to perform FTP transfers and upload files at the specified folder location on the iSPI for IP Telephony server. Make sure that you specify the same relative path to the directory name (directory on the iSPI for IP Telephony where the CDR files are uploaded by the CDR repository node in the cluster) in the Cisco CDR Data Access Configuration page in the iSPI for IP Telephony while configuring CDR access for the cluster.

- The CDR-on-Demand Web Service-based collection requires you to specify the following details:

  — The SOAP/Web-Services user name and password

  — The IP address or the fully qualified domain name of the call manager server node on the cluster that hosts the CDR-on-Demand Web Service. The iSPI for IP Telephony requires you to set up the FTP server on the iSPI for IP Telephony in such a way that the home directory of the FTP user is a valid sub directory under the `$NnmDataDir/log/ipt/tmp` directory. Make sure that the CDR repository hosting node in the cluster has adequate ability to perform FTP transfers and upload files at the specified folder location on the iSPI for IP Telephony server.

- Specify the time interval at which the iSPI for IP Telephony server must scan the billing server directory for newly arriving CDR or CMR files. If you are using the CDR-on-Demand Web Service method, specify the time interval at which the iSPI for IP Telephony server must look for newly created CDR or CMR files by using the CDR-on-Demand Web Service. It is recommended that you specify a time interval of two minutes to five minutes for scalable processing of the CDR or CMR information across a period of time. It is also recommended that you configure the CDR repository server node in the cluster to publish the CDR or CMR files after short time intervals instead of publishing the accumulated CDR or CMR information after a time interval of two minutes to five minutes.

Avaya Data Access Recommendations

Make sure that you configure all the primary communication managers and Local Survivable Processors (LSP) as valid sources of CDR data. In the case of duplex pair of primary communication managers, make sure that you configure the CDR data access for both the primary communication managers in the pair.

Note down the following details for each of the communication managers in your deployment and provide the same information in the Data Access Configuration form provided by the iSPI for IP Telephony:

- The format of the CDRs used by the communication manager. You can retrieve the information about the format of CDRs from the appropriate SAT screen on the native configuration manager of the selected communication manager. For more information, see the Avaya Communication Manager documentation or contact the administrator of such communication manager servers.
- The time-zone of the communication manager.
- The date format for the month and the day in the date fields of CDRs from the communication manager. The format might be in the MMDD or the DDMM format. You can obtain this information for a specific communication manager from the appropriate SAT screen on the native configuration manager of the selected communication manager. For more information, see the Avaya Communication Manager documentation or contact the administrator of such communication manager servers.
- Note whether the circuit ID fields for the trunk group members appear in the CDRs. You must also note if the circuit ID is modified while the CDRs are populated by the CM, and if the circuit ID fields must be interpreted in a way to re-construct the appropriate circuit ID. You can retrieve this configuration flag from the appropriate SAT screen on the native configuration manager of the communication manager. For more information, see the Avaya Communication Manager documentation or contact the administrator of such communication manager servers.
- The iSPI for IP Telephony supports collection of CDR using one of the following methods:
  - File-based survivable CDR collection
  - Accessing CDRs pushed through a TCP/IP link using the Reliable Session Protocol

    You must determine the mode used by a specific communication manager before proceeding with the remaining configuration tasks for CDR data access.
- Verify the following points:
  - Check if the survivable CDR feature is enabled for the communication manager.
  - Check if the communication manager is configured to periodically write files containing CDR information at the designated location on the communication manager.

  If the verification is true for both the listed points, then, you must supply the valid SFTP user name and password to access the CDR directory on the communication manager that contains the CDR files. Make sure that you work with administrator for the communication manager and to get the appropriate SFTP user created and CDR access turned on at the communication manager. You can retrieve the information about the survivability of CDRs from the appropriate SAT screen (system-parameters cdr) on the native configuration manager of the communication manager. For more information, see the Avaya Communication Manager documentation or contact the administrator of such communication manager servers.

- If you have not configured survivable CDRs for the communication manager and if the CDRs are pushed through a TCP/IP link using the Reliable Session Protocol, then, you must do additional configuration using the SAT screen on the native configuration manager of the communication manager. Using this configuration, you must create a valid Avaya node name linked to the IP Address of the iSPI for IP Telephony server where you want the CDRs to be pushed by the communication manager. You must also do the IP-services configuration to specify the previously configured node name as the CDR link peer and specify the TCP/IP port number on the iSPI for IP Telephony server where you want the CDRs to be sent. Note down the other Reliable Session Protocol (RSP) settings such as the Packet Response Timer and the Inactivity Timer as they are configured in the IP-services SAT screen. You must specify the same values in the Avaya CDR Data Access configuration page for the iSPI for IP Telephony. Note that you must set the Reliable flag to `true` in the IP-services SAT screen as the iSPI for IP Telephony only works with the communication manager acting as an RSP peer while sending the CDR data through a TCP/IP link. Depending on whether the communication manager is configured to send CDRs directly to the iSPI for IP Telephony or through a CLAN device, specify the CLAN IP address in the Avaya CDR Data Access configuration page of iSPI for IP Telephony. You can retrieve the information about the survivability of CDRs from the appropriate SAT screen on the native configuration manager of the communication manager. For more information, see the Avaya Communication Manager documentation or contact the administrator of such communication manager servers.
- If the communication manager uses customized CDR format, then you must create the format specification file, save it on the disk of your iSPI for IP Telephony server, and specify the absolute path to the format specification file while configuring Avaya CDR data access using the iSPI for IP Telephony. It is recommended that the format specification file is saved in specific folders on the iSPI for IP Telephony server. This makes sure of implementing consistency in the Avaya CDR processing-based features in the iSPI for IP Telephony deployed in an Applicable Failover or HA environment. The designated folder where the iSPI for IP Telephony saves the format specification file is as follows: `$NnmDataDir/shared/ipt/avayacdr/conf`. You must also make sure that you create a format specification file for each communication manager which has a different customized CDR format. You must specify the absolute path to the file when configuring CDR data access for individual communication managers using the iSPI for IP Telephony. In case multiple communication managers have the same customized CDR format, then, you can specify the absolute path to the same customized format specification file while configuring CDR data access for each of these communication managers.

The iSPI for IP Telephony supports standard or customized CDR formats for Avaya IP Telephony. The iSPI for IP Telephony supports the following standard formats:

- 59 character
- Printer
- TELESEER
- ISDN-Printer
- ISDN-TELESEER

For customized CDR format, you can see the `NnmDataDir/shared/ipt/conf/CustomizedCDRFormat.properties` file and configure this file as required. You can refer to the instructions in this file to modify this file. You must make sure that you do not include blank space characters before or after the changes you make.

You must provide the following details to configure CDR access for Avaya:

- 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 standard CDR formats supported.
- 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.

You must not edit the standard CDR format 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. You can specify the time zone if the communication manager and the iSPI for IP Telephony server are in different time zones. If you do not provide a time zone value, the iSPI for IP Telephony uses the time zone configured for the iSPI for IP Telephony server.

Configuring Avaya RTCP Reception

To monitor the voice quality at the Avaya RTP endpoints during a call and to generate reports on the voice quality, the iSPI for IP Telephony relies on the reception and processing of RTCP packets from Avaya RTP endpoints such as the IP phones, the media processors, and the H.248 gateways. To enable the iSPI for IP Telephony to process the RTCP packets from the Avaya RTP endpoints, you must configure the reception of RTCP packets using the Data Access Configuration form provided by the iSPI for IP Telephony. You can perform this configuration by logging on to the NNMi console as an administrator.

The points to consider while configuring Avaya RTCP reception are as follows:

- You must make sure that you perform the required configuration tasks on the Avaya Communication Managers using the support SAT screens in the native configuration UI. You must specify the IP address and the port number of the RTCP server to be used as the destination for a copy of the RTCP packets sent by the Avaya RTP session participants to other session participants. Make sure that you configure the endpoints of the primary communication managers appropriately to send the RTCP packets to the iSPI for IP Telephony.
- You must make sure that all the endpoints included in the network region on the communication manager use the same default RTCP server settings (the same IP address and UDP port number combination that maps to a valid IP address and UDP port number on the iSPI for IP Telephony server.
- You must also make sure to specify the correct IP address and the UDP port number combination in the Data Access Configuration form for the iSPI for IP Telephony. Make sure to specify the same values that you had specified in the native configuration wizard

for the communication manager for receiving and processing the RTCP packets at the iSPI for IP Telephony server. You must provide the required details for all the fields in this form.

- If you had seeded the node hosting a primary communication manager using an iSPI for IP Telephony instance, then make sure that you do the required configuration first on the communication manager and then on the iSPI for IP Telephony. This makes sure that the copies of RTCP packets sent from the endpoints of the communication manager are received by the iSPI for IP Telephony instance used to seed the node hosting the primary communication manager.

Opening Firewall Ports

Based on the type of IP telephony infrastructure that you monitor in your enterprise, you must open a few ports to enable communication through firewalls.

Cisco IP Telephony

If you monitor a Cisco IP telephony infrastructure in your enterprise, you must open the following ports in the NNMi management server:

Table 1

Port Number	Protocol	Comments
162	SNMP over UDP	This port is used for receiving SNMP traps from the devices.
21	FTP over TCP	This port is used for CDR push using FTP from Cisco Unified Communications Manager clusters; specifically from the publisher Cisco Unified Communications Manager in the cluster.

You must also open the following ports in the relevant Cisco IP telephony entities:

Table 2

Port Number	Protocol	Comments
161	SNMP over UDP	This port is used for sending SNMP queries to the Cisco devices to collect data from them. Open this port in the relevant IP telephony devices such as Cisco Unified Communications Managers, Cisco Unified Communications Manager Expresses, voice gateways, gatekeepers, SRST routers, unity connections, unity devices, and so on.
8443	SOAP/HTTPS over TCP	This port is required by NNM iSPI for IP Telephony to collect essential configuration and CDR data by communicating with the CDRonDemand Web services serviceability interface and AXL Web services serviceability interface on Cisco Unified Communications Manager cluster. Open this port in the publisher Cisco Unified Communications Manager in the Cisco Unified Communications Manager cluster.
22	SSH over TCP	This port is required by NNM iSPI for IP Telephony to execute UCOS CLI commands programmatically on the Cisco Unified Communications Manager nodes. Open this port in all Cisco Unified Communications Managers in the Cisco Unified Communications Manager cluster.
80	HTTP over TCP	This port is required for the programmatic collection of Quality of Experience (QoE) measures for active RTP sessions and audio calls in which the Cisco IP phones take part. Open this port in all Cisco IP phones controlled by various Cisco Unified Communication Manager clusters. You can decide not to open this port in the phones for which you want the real time monitoring of QoE measures, such as MOS, jitter, latency, and delay.

Avaya IP Telephony

If you manage an Avaya IP telephony infrastructure in your enterprise, you must open the following ports in the NNMi management server:

Table 3

Port Number	Protocol	Comments
162	SNMP over UDP	This port is used for receiving SNMP traps from the Avaya Communication Managers.
Configurable	RTCP over UDP	Configure a port for RTCP packets reception in the NNMi management server for each Avaya Communication Manager. The ports must be distinct for each Avaya Communication Manager. You cannot use the same port for two or more Avaya Communication Managers. The Avaya RTP endpoints (such as IP Phones, media gateways, and media processors) controlled by an Avaya Communication Manager send the RTCP packets to the port configured for that particular Avaya Communication Manager. If the primary Avaya Communication Manager is deployed in duplex redundant pair, you need to open this port in only one of the two physical Avaya Communication Managers.
Configurable	Avaya RSP over TCP	Configure a port for Avaya Reliable Session Protocol (RSP) in the NNMi management server for each Avaya Communication Manager. You must not use the same port for more than one Avaya Communication Manager. Each Avaya Communication Manager streams the CDRs to the port configured for this purpose. An Avaya Communication Manager may stream CDRs to this port directly or through its Processor Ethernet IP node or CLAN IP node. If the primary Avaya Communication Manager is deployed in duplex redundant pair, you need to open this port in only one of the two physical Avaya Communication Managers.

You must also open the following ports in the relevant Avaya IP telephony entities:

Table 4

Port Number	Protocol	Comments
161	SNMP over UDP	This port is used for sending SNMP queries to the Avaya devices to collect data from them. Open this port in the relevant IP telephony devices such as Avaya Communication Managers, Local Survivable Processors (LSPs), H248 media gateways, CLANs, and so on.
5022	SSH over TCP	This port is required by NNM iSPI for IP Telephony to execute Avaya SAT commands programmatically on the Avaya Communications Manager servers. Open this port in both physical Avaya Communication Managers in redundant pairs.
22	SSH over TCP	This port is required for the programmatic execution of sftp/ssh to collect CDR files from Avaya Communication Managers. Open this port in both physical Avaya Communication Managers in redundant pairs. Open this port only if the Avaya Communication Manager streams its CDR data using RSP. If the Avaya Communication Manager provides the CDR data through survivable file based CDR interface, you may not have to open this port.

Microsoft IP Telephony

If you monitor a Microsoft IP telephony infrastructure in your enterprise, you must open the port mentioned below in the NNMi management server:

Table 5

Port Number	Protocol	Comments
162	SNMP over UDP	This port is used for receiving SNMP traps from the devices.

You must also open the following ports in the relevant Microsoft IP telephony devices:

Table 6

Port Number	Protocol	Comments
161	SNMP over UDP	This port is used for sending SNMP queries to the Sangoma gateways and NET gateways to collect data from them. Open this port in the Sangoma gateways and NET gateways.
1433	TCP	This port is used for CDR/QOE data collection from the monitoring server database. The default port is 1433, but you can configure any other port also for this purpose. Open this port on each server in the monitoring server pool.
1434	UDP	This port is used for CDR/QOE data collection from the monitoring server database. Open this port on each server in the monitoring server pool.
5985/5986(Http/ Https)	TCP	These ports are used for initiating remote powershell commands on Lync FrontEnd server. Open these ports on each server in the Lync FrontEnd server pool.

Configuring Reporting Data Retention Period

After integrating the iSPI for IP Telephony with the iSPI Performance for Metrics/Network Performance Server for reporting, you can configure the reporting data retention period. You can configure this value while installing the Network Performance Server. You can also modify the data retention period using the configuration utility provided by the Network Performance Server. See the *HP Network Mode Manager i Software Smart Plug-in for Metrics Installation Guide* for more information.

Setting Up the Shared Directory for Network Performance Server

When installed on a dedicated server, the Network Performance Server (NPS) creates a shared directory on the NNMi management server to gather the data collected by NNMi. You must make sure that the shared directory is present before using the iSPI for IP Telephony and the iSPI Performance for Metrics/Network Performance Server to view reports. See the *HP Network Mode Manager i Software Smart Plug-in for Metrics Installation Guide* for more information about creating the shared directory.

7 Troubleshooting

Discovery of Avaya Communications Manager Server Fails

To resolve this issue, perform the following tasks:

Task 1: Create Communication Configuration Regions for Avaya Communication Manager

Task 2: Configure IP Address for SNMP Access on Avaya Communication Manager

Task 3: Configure SNMP Communities on Avaya Communication Manager

Task 4: Configure the Discovery Cycle for Avaya

Task 1: Create Communication Configuration Regions for Avaya Communication Manager

Specify the communication configuration for Avaya Communication Manager servers: it is recommended that SNMP queries do not use `SNMP GetBulk` while communicating with these nodes. To enforce this restriction and consistent behavior of SNMP agents on the Avaya Communications Manager server nodes, use the Communication Configuration form in the NNMi Configuration workspace and specify Regions that include this exclusive specification of communication configurations only for the required set of Avaya Communications Manager Server nodes. Note that you will have to complete this configuration task for all the Avaya Communications Manager server nodes, including each physical server in duplex redundant pairs of Primary Servers, each stand-alone Primary Server that is not deployed in duplex redundant pairs, and each Local Survivable Processor (LSP) server node in your environment. For better consistency in request response sessions, it is also recommended that you set up the regions in such a way that NNMi and iSPI for IP Telephony use a time-out value of 59 seconds and retry count value of 1 for all SNMP communications with these nodes. For more information on specifying Regions, see the *NNMi Online Help for Administrators*.

Task 2: Configure IP Address for SNMP Access on Avaya Communication Manager

You must make sure that Avaya Communication Manager receives SNMP requests only from the NNMi management server. You can make sure this by configuring the IP address of NNMi management server alone for SNMP access in the System Management Interface (SMI) window of the Avaya Communication Manager. For more information, see the Avaya Communication Manager documentation.

Task 3: Configure SNMP Communities on Avaya Communication Manager

You must enable both SNMP Version 1 and SNMP Version 2c in the Avaya Communication Manager. You must also configure the same Community Name (read-only) for SNMP Version 1 and SNMP Version 2c.

Task 4: Configure the Discovery Cycle for Avaya

If you continue to face this issue, you must configure the discovery cycle for Avaya as follows:

1. In the Discovery Configuration form, clear the **Use NNMi node discovery interval?** check box.
2. Type the **Discovery Interval** in hours. The default interval is 2160 hours (90 days). The recommended discovery interval is 2160 hours.
3. Select **Pause state pollers during discovery?** check box.

You must install the following Avaya service packs (patches) on the Avaya Communication Managers before you configure the discovery cycle for Avaya:

- Service pack 6 (Patch 18576) or later versions of the service packs if you are using version 5.x of the Avaya Communication Manager.
- Service pack 2 (Patch 18567) or later versions of the service packs if you are using version 6.x of the Avaya Communication Manager.

For more information on *Configuring Discovery Cycle for Avaya Primary Servers*, see the *NNM iSPI for IP Telephony Online Help for Administrators*.

SNMP Request to Nortel Devices Times Out.

To resolve this issue and for the consistent behavior of SNMP agents on the Nortel nodes, use the **Communication Configuration** form in the NNMi Configuration workspace and specify **Regions** only for the Nortel nodes.

For better consistency in request response sessions, follow these steps:

- Set up the regions in such a way that NNMi and NNM iSPI for IP Telephony use a time-out value of 59 seconds and retry count value of 2
- Use SNMPv1 for all communications with these nodes.

For more information on specifying Regions, see the *NNMi Online Help for Administrators*.

SNMP Trap Loading Fails for Avaya and Nortel Devices

NNMi fails to load the NNM iSPI for IP Telephony specific SNMP traps if you have `Avaya G3 Alarms` and/or `Nortel COMMON MIB` SNMP traps loaded before you install the NNM iSPI for IP Telephony.

Cause:

NNMi fails to load the NNM iSPI for IP Telephony specific SNMP traps because the traps with same SNMP Object ID are loaded in the NNMi database. This results in the "`duplicate key - unique constraint violation`" exception.

Symptom:

Symptom can be any one of the following:

- The NNM iSPI for IP Telephony workspace is not available.
- The `%NnmDataDir%\log\nnm\nnm-trace.log` file contains trace messages similar to following message:

```
ERROR: duplicate key value violates unique constraint
"nms_snmp_trap_config_oid_key"
```

Solution:

If you have any `Avaya G3 Alarm` SNMP traps loaded before installing the NNM iSPI for IP Telephony, follow these steps:

1. Log on to the NNMi console.
2. From the Workspace pane, click **Configuration** and expand **Incidents**.
3. Click **SNMP Trap Configurations**. The SNMP Trap Configurations view opens in the right pane.
4. Select the SNMP traps with the following `SNMP Trap Object ID (OID):`
   - `.1.3.6.1.4.1.6889.1.8.1.0.2`
   - `.1.3.6.1.4.1.6889.1.8.1.0.3`
   - `.1.3.6.1.4.1.6889.1.8.1.0.4`
   - `.1.3.6.1.4.1.6889.1.8.1.0.5`
   - `.1.3.6.1.4.1.6889.1.8.1.0.6`
   - `.1.3.6.1.4.1.6889.1.8.1.0.12`
   - `.1.3.6.1.4.1.6889.1.8.1.0.14`
   - `.1.3.6.1.4.1.6889.1.8.1.0.15`
5. Click **Delete**.
6. Restart the `ovjboss` process by running the following commands:
   a. **`ovstop -c ovjboss`**
   b. **`ovstart -c ovjboss`**

If you have any `Nortel COMMON MIB` SNMP traps loaded before installing the NNM iSPI for IP Telephony, follow these steps:

1. Log on to the NNMi console.
2. From the Workspace pane, click **Configuration** and expand **Incidents**.
3. Click **SNMP Trap Configurations**. The SNMP Trap Configurations view opens in the right pane.
4. Select the SNMP traps with the following `SNMP Trap Object ID (OID)`
   - `.1.3.6.1.4.1.562.3.10.10.1.0.1`
   - `.1.3.6.1.4.1.562.3.10.10.1.0.2`
   - `.1.3.6.1.4.1.562.3.10.10.1.0.3`
   - `.1.3.6.1.4.1.562.3.10.10.1.0.4`
   - `.1.3.6.1.4.1.562.3.10.10.1.0.5`
   - `.1.3.6.1.4.1.562.3.10.10.1.0.6`
   - `.1.3.6.1.4.1.562.3.10.10.1.0.7`
5. Click **Delete**.
6. Restart the `ovjboss` process by running the following commands:
   a. **`ovstop -c ovjboss`**

b **ovstart -c ovjboss**

Measurement Type for a UCM Cluster show 'No Value' in the Analysis Pane

One or more Measurement Type for a UCM Cluster may show `No Value` in the Analysis Pane.

Cause:

This may happen because one of the UCM is not responding or not collecting data for the particular Measurement Type.

Symptom:

Value of Measurement Type in the Analysis Pane for a UCM cluster is `No Value` in the UCM Clusters view.

Solution:

To resolve this problem, follow these steps:

1. Log on to the NNMi console.
2. Click **Cisco IP Telephony**.
3. Click **UCM Clusters**.
4. Double-click the UCM Cluster that you want to verify. The UCM Cluster Details form opens.
5. Click **UCMs** tab in the right pane. The UCMs view opens on the right pane.
6. Verify each UCM listed in the UCM cluster.
   a. You must verify which UCM is not responding to data collection request for the Measurement Type that is showing `No Value`.
   b. You can check if there is any SNMP or SSH access issue for the particular UCM.

A Performance and Scalability Metrics for the iSPI for IP Telephony

You can use the following performance and scalability metrics to plan the deployment of the iSPI for IP Telephony in your enterprise.

The performance and scalability metrics values for a single instance deployment of the iSPI for IP Telephony are as follows.

Entity	Count	Additional Information
IP phone extensions and associated IP telephony functions/devices	Up to 50,000	You can include devices from different vendors. Note that the device count stays below 50,000. It is assumed that the count of the remaining NNMi objects (routers, switches, nodes, and so on) is less than 3500. In a Global Network Management (GNM) environment, the iSPI for IP Telephony supports up to 2,50,000 IP phone extensions and associated IP telephony functions/devices.
Host Channel Adapter (HCA)/Horizontal Cross Connect (HCC) sustained with 100,000 Busy Hour Call Attempts (BHCA)/ Busy Hour Call Completion (BHCC) for CDR collection, analysis and reporting on Call Duration, Call Counts, Call Quality Metrics Jitter, Packet Loss, Delay and MOS.	Up to 53,000	Call Quality Metrics reporting is available only for Cisco in the 9.01 version of the iSPI for IP Telephony. The reporting data is retained for a period of 70 days. In a Global Network Management (GNM) environment, the iSPI for IP Telephony supports up to 5,30,000 HCA/HCC sustained with 100,000 BHCA/BHCC for CDR collection, analysis and reporting.
User sessions	Up to 40	Support for up to 40 simultaneous user sessions

Entity Discovered	Discovery Time	Additional Information
Discovery of IP telephony entities and the corresponding configuration properties required for subsequent monitoring and diagnostics	24 hours	After the discovery is complete, the iSPI for IP Telephony completes the initialization of the states and the current values of hourly performance and usage metrics from the network within 30 minutes.
Detect state changes for IP telephony entities after discovery and initialization	Within 10 minutes	For the IP phone entities, you can configure the iSPI for IP Telephony to detect changes in registration states within five minutes.
Alerts for breach of set thresholds for Cisco IP Telephony Call Quality metrics (Jitter, Packet Loss, Delay and MOS)	Within five minutes	The alert is generated within five minutes of call completion.
Alerts for breach of set thresholds for Avaya IP Telephony hourly performance and usage measures such as Call Processor Occupancy Summaries, Port Network Load Summaries, DSP/CODEC Usage Summaries, Route Pattern/Trunk Group Usage Summaries, and so on	Within 30 minutes	The alert is generated within 30 minutes of threshold violation.

See the i*SPI for IP Telephony Support Matrix* for more information. You can contact HP Support or see the *NNMi Support Matrix* and the *iSPI Performance for Metrics Support Matrix* for more information to assist you in sizing your NNMi and iSPI Performance for Metrics/Network Performance servers adequately to support the highest sustained demands on scalability and performance.

B Proxy Service for Microsoft IP Telephony

The `msproxy` service that you create (using the procedure listed in the *Creating the Proxy Service* section in the *iSPI for IP Telephony Installation Guide*) acts as the communication interface between the iSPI for IP Telephony and the Microsoft Lync server. All the requests (such as topology discovery, CDR collection, and so on) from the iSPI for IP Telephony pass through this service to the Microsoft Lync server.

During startup, the `iptjboss` process connects to the `msproxy` service using the port number defined in the `msipt.proxy` file present in the `%nnminstalldir%\shared\ipt\conf` directory.

The `msipt.proxy` file includes the following parameters that the `iptjboss` process uses to connect to the `msproxy` service:

- Address: Indicates the IP address at which the `msproxy` service is running. By default, the proxy service runs on the local host.
- Port: Indicates the port number used by the msproxy service. The service uses the port number 8000 by default. If this port number is already in use, you must change the port number for the proxy service as listed in the *Changing the Port of the Proxy Service* in the *iSPI for IP Telephony Installation Guide*.
- RequestThreads: Indicates the maximum number of request threads handled by the proxy service at point of time. This is configured to five, by default.
- ResponseThreads: Indicates the number of response threads handled by the proxy service at a point of time. This is configured to five, by default.

Apart from changing the port number if required, it is recommended not to change the values of the other listed parameters.

You can use the following commands to start, stop, and check the status of the msproxy service:

- **`ovstart - c msproxy`**
- **`ovstop - c msproxy`**
- **`ovstatus - c msproxy`**

We appreciate your feedback!

If an email client is configured on this system, click Send Email

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

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

Document title: Deployment Guide

Feedback:


Java
COMPATIBLE