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

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

Software Version: 9.00

Installation Guide

Document Release Date: March 2010
Software Release Date: March 2010

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 Notices

Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

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

Java™ is a US trademark of Sun Microsystems, Inc.

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

Oracle® is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group

Oracle Technology — Notice of Restricted Rights

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

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

Printed in the U.S.

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 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 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 Introduction

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

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

- Automatically discovering of the IP Telephony infrastructure
- Monitoring the states related to fault and usage of various discovered components of the IP telephony infrastructure
- Reporting on the call metrics (CDR data for Avaya and Cisco IP Telephony)

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

The iSPI for IP Telephony works with NNMi to introduce additional views and forms that help you view and analyze the data collected from the discovered IP telephony network. While NNMi presents the framework to monitor the state of the network and computing environment in your organization, the IP telephony-specific views, which are introduced in the NNMi console by the iSPI for IP Telephony, help you monitor the health and performance of the IP telephony network. With the operator-level access, you can view the data collected and displayed by the iSPI for IP Telephony to monitor the health, performance, and availability of the IP telephony network. With the administrative access, you can configure the details such as monitoring interval for monitoring tasks, various data access configurations required, various thresholds for monitoring, and so on.

This version of the iSPI for IP Telephony supports Cisco, Avaya, and Nortel IP Telephony networks.

IP Telephony Workspaces

The iSPI for IP Telephony introduces three new workspaces in the Workspaces pane in the NNMi console: **Cisco IP Telephony**, **Avaya IP Telephony**, and **Nortel IP Telephony**.

These workspaces present gateways to view all the details indicating the health, performance, and availability of the Cisco, Avaya, and Nortel IP Telephony network with the help of the different views. Every view lists the details of the discovered devices that indicate the states and properties of the devices. You can view additional details of every device listed in a view with the help of forms.

Related Documentation

See the following guides for more information on iSPI for IP Telephony:

- **iSPI for IP Telephony Online Help**—includes information on the views and forms introduced by the iSPI for IP Telephony.
- **iSPI for IP Telephony Release Notes**
- **iSPI for IP Telephony Support Matrix**

2 Before You Begin

Before you start installing the iSPI for IP Telephony, you must plan the installation based on your deployment requirements. You must identify the ideal deployment scenario among the supported configurations, make sure that all the prerequisites are met, and then begin the installation process.

You can refer to the following documents before you start the installation process:

- *HP Network Node Manager i Software 9.00 Installation Guide for Windows* or *HP Network Node Manager i Software 9.00 Installation Guide for UNIX*
- *HP Network Node Manager i Software 9.00 Deployment Reference Guide*
- *HP Network Node Manager i Software 9.00 Release Notes*
- *HP Network Node Manager i Software 9.00 Support Matrix*
- *HP Network Node Manager i Software Smart Plug-in Performance for Metrics/NPS Installation Guide*
- *HP Network Node Manager i Software Smart Plug-in Performance for Metrics/NPS Support Matrix*
- *HP Network Node Manager i Software Smart Plug-in Performance for Metrics/NPS Release Notes*

Before you begin, make sure that NNMi is installed in the environment and running. You must install the iSPI for IP Telephony on the NNMi management server. You can also install the iSPI in High-Availability (HA) cluster environments that are supported by NNMi.

Installation Plan on the NNMi Management Server

Before installing the iSPI for IP Telephony on the NNMi management server, you must note down all the configuration related details of the NNMi installation. These details will be required by the iSPI installer.

Database Details

NNMi installer installs a default database that is embedded with the product. However, to achieve higher scalability, you can choose an external Oracle database instead of the embedded database to store NNMi data. See the *HP Network Node Manager i Software 9.00 Installation Guide* for more information on configuring NNMi with Oracle. You must note down the following details of the NNMi database:

- **Type:** The default embedded database or Oracle.
- **Port:** *Only for Oracle.* The port used by the Oracle database.
- **Hostname:** *Only for Oracle.* This is applicable when you use an Oracle database residing on a remote server. Note down the fully-qualified domain name of the database server.
- **Database name:** *Only for Oracle.* Name of the Oracle database instance.
- **User name:** *Only for Oracle.* The Oracle user name created to access NNMi data.
- **Password:** *Only for Oracle.* Password of the above user.

With the iSPI for IP Telephony, you must use a unique Oracle instance, and not the Oracle instance configured with NNMi. Before you create a unique Oracle instance for the iSPI, refer to the *Database Installation* section in the *HP Network Node Manager i Software Installation Guide* for additional details. If you are using a unique Oracle instance, note down the aforementioned details for this instance as well.

NNMi Installation

You must make sure that NNMi is installed and running on the machine where you plan to install the iSPI for IP Telephony.

iSPI Performance for Metrics/NPS

You must make sure that the iSPI Performance for Metrics/NPS is running if this application is a part of your deployment environment.

Check System Requirements

Make sure the management server meets all the hardware and software requirements.

Refer to the *HP Network Node Manager i Software Smart Plug-in for IP Telephony Support Matrix* and *HP Network Node Manager i Software Smart Plug-in for IP Telephony Release Notes* documents for a complete information on hardware and software requirements and dependencies.

Table 1 Preinstallation Checklist for Hardware and Software Requirements

Requirement	Reference Document	Complete? (Yes/No)
Disk space	*HP Network Node Manager i Software Smart Plug-in for IP Telephony Support Matrix*	
Operating system	*HP Network Node Manager i Software Smart Plug-in for IP Telephony Support Matrix*	
Database	*HP Network Node Manager i Software Smart Plug-in for IP Telephony Support Matrix*	
Browser	*HP Network Node Manager i Software Smart Plug-in for IP Telephony Support Matrix*	

Preinstallation Tasks

Before you begin installation, perform these tasks:

Task 1: Create a New User with the Web Service Client Role

Create a user from the NNMi console with the Web Service Client role. This user will be used during the course of installation.

Do not use the NNMi **system** account while installing the iSPI for IP Telephony.

Task 2: *Only for Oracle.* Create a New Oracle Instance

Skip this task if you choose to use the embedded database. You must create a new Oracle instance before installing the iSPI for IP Telephony. While installing and configuring the iSPI for IP Telephony, do not use the same Oracle instance that was configured with NNMi.

Task 3: Configuration Tasks on NNMi

Perform the following configuration tasks on NNMi before installing the iSPI for IP Telephony:

- Automatic discovery rules: It is recommended that you setup the auto-discovery rules for discovery of non-SNMP nodes that host IP Phones in your network. You can do this by using the Discovery Configuration form in the NNMi Configuration workspace and adding the auto-discovery rules. You must specify the auto-discovery rules in a manner that covers the range of IP addresses for all the possible IP addresses of the IP Phones in your environment. For more information about specifying automatic discovery rules, see the *NNMi Online Help for Administrators*.
- Specify the SNMP v1/v2 community strings: Obtain the SNMP v1/v2 read community strings for all the IP Telephony nodes (for example, the Avaya Communication Manager Server nodes, the Avaya LSP nodes, the Avaya Media Gateway nodes, the Cisco Unified Communications Manager nodes, the Cisco Voice Gateway nodes, the Cisco SRST nodes, the Cisco Call Manager Express nodes and so on). Use the Communication Configuration form in the NNMi Configuration workspace to add these community strings in list of default read community strings to be used by

NNMi and iSPI for IP Telephony for SNNP v1/v2-based communication. For more information about specifying SNMP v1/v2 community strings, see the *NNMi Online Help for Administrators*.

- Specify the communication configuration for Avaya Communication Manager servers: It is recommended that NNMi and the iSPI for IP Telephony is configured to use either SNMP v1 or SNMP v3 for communication with Avaya Communications Manager server nodes in your deployment environment. It is also 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 desired 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*.

3 Installing the iSPI for IP Telephony

You can install the iSPI for IP Telephony on both types of management servers—Windows and UNIX. You can use the installation wizard. The installation wizard guides you through the installation process.

If you are updating the iSPI for IP Telephony from earlier versions, see the *HP NNM i Software Smart Plug-in for IP Telephony Deployment Guide*. for information on upgrade instructions.

Installing on a Windows or UNIX Management Server

To install the iSPI for IP Telephony on a Windows or UNIX management server, follow these steps:

1. Log on to the management server with the `Administrator` privileges.
2. Insert the iSPI installation CD into the CD-ROM drive.
3. In the root directory, double-click the `setup.exe` file (for Windows) or the `setup.bin` file (for UNIX and Linux). The installation wizard opens.
4. In the Introduction screen of the installation wizard, click **Next**. The License Agreement screen appears.
5. In the License Agreement screen, select the **I Accept...** option, and then click **Next**. The Product Customization screen appears.
6. Select one of the following options from the **Choose the database type** section on the Server Configuration page and click **Next**:
   - **HP Software Embedded Database**
   - **Oracle**

7 If you selected **Oracle** in the previous step, you must specify the following details in the screens that follow. You can go to *step 8* if you selected the **HP Software Embedded Database** option:

— Database Initialization Preferences: Select **Primary Server Installation** or **Secondary Server Installation** based on what you have configured for NNMi installed on this system.

— Database Server Information to Connect to: Specify the following details to connect to the Oracle database server you have configured for NNMi:

– **Host**: The fully-qualified domain name of the Oracle server.

– **Port**: The port number used by the Oracle database server.

– **Instance:** Name of the Oracle instance that you want to use with the iSPI for IP Telephony.

You must create an Oracle instance apart from the instance configured for NNMi. Do not use the same Oracle instance that was configured with NNMi.

— Database User Account Information: specifies the user account information required to access the Oracle database. you must specify the following details:

– **Username**: User name to access the Oracle database instance.

– **Password**: Password for the specified user name.

8 Click **Next**. The Install Checks screen appears. The wizard checks for the available disk space.

9 After the check is complete, click **Next**. The Pre-Install Summary screen appears.

10 Review the options, and then click **Install**. The installation process begins.

Perform a forced reinstallation of the already installed components if you previously attempted an unsuccessful installation of the iSPI for IP Telephony and you did not manually removed the components that were already placed by the installer

11 Specify the following details:

- **Information required by the iSPI for IP Telephony to communicate with NNMi**

- NNMi FQDN—the Fully Qualified Domain Name (FQDN) for the NNMi management server.
- NNMi HTTP Port—the NNMi HTTP port number.
- NNMi HTTPS Port - the NNMi HTTPS port number.
- NNMi JNDI Port—the NNMi JNDI port number

- The iSPI for IP Telephony installer detects the values listed above based on the values currently used by NNMi.
- If the values listed above are modified by the NNMi administrator after the installation of the iSPI for IP Telephony, you must reconfigure the iSPI for IP Telephony to use these updated values. See section Configuring iSPI for IP Telephony to Use Modified NNMi Ports on page 29 for detailed instructions.

  - Web Service Client Username—specify the NNMi Web Service Client user name. Use the Web Client user you created.
  - Web Service Client Password—password for the above user.
  - Retype Password - Retype the password to confirm the password.

- If you want to use a different user name or if you change the password after installation of the iSPI for IP Telephony, you must reconfigure the iSPI for IP Telephony to use these updated values. See section Configuring iSPI for IP Telephony to Use Modified NNMi Web Services Client User Name and or Password on page 30 for detailed instructions.

  - isSecure - Select the option to enable HTTPS. By default, the iSPI for IP Telephony uses HTTP to communicate with NNMi.

- If you want to change your mode of communication after installation of the iSPI for IP Telephony see section Updating the Security Mode (HTTP to HTTPS) on page 28 for detailed instructions.

  - **Information required by NNMi to Communicate with iSPI for IP Telephony**
    - IPT FQDN—the fully-qualified domain name of the iSPI for IP Telephony.
    - IPT HTTP Port—the HTTP port of the iSPI for IP Telephony.
    - IPT HTTPS Port—the HTTPS port of the iSPI for IP Telephony.

— IPT JNDI Port—the JNDI port of the iSPI for IP Telephony.

The iSPI for IP Telephony installer displays the default values for the ports listed above. You can specify the values of your choice. If you want to modify these values after installing the iSPI for IP Telephony, see section Modifying iSPI for IP Telephony Ports on page 31 for detailed instructions.

— isSecure - Select the option to enable HTTPS. By default, NNMi uses HTTP to communicate with the iSPI for IP Telephony. .

- If you want to change your mode of communication after installation of the iSPI for IP Telephony see section Updating the Security Mode (HTTP to HTTPS) on page 28 for detailed instructions.

The various cases for the (Fully Qualified Domain Name (FQDN) configuration parameters are listed below:

- The NNMi and iSPI for IP Telephony must use the same FQDN. If the NNMi server has more than one domain name, the NNMi installation process sets one FQDN and the iSPI for IP Telephony installation also must use the same domain name. To find the official FQDN of the NNMi server, use any *one* of following:

  — Run the **`nnmofficialfqdn.ovpl`** command.

  — From the NNMi console, click **Help > About Network Node Manager i Software.**

- At the time of NNMi installation, if you are using the partial domain name as <people> or the IP Address as <xx.xx.xx.xx> and not the fully qualified domain name, the Single Sign-on feature is disabled.

12 Click **OK**.

13 This displays the Configuring IPT SPI dialog box to enable the integration with the iSPI Performance for Quality Assurance. If you want to enable this integration, select the check box and specify the following details. Click **Skip** if you do not want to enable this integration now:

— **Host Name**: specify the host name for the machine that hosts the iSPI Performance for Metrics/NPS integrated with the iSPI Performance for Quality Assurance.

— **Port Number**: specify the port number used by the iSPI Performance for Metrics/NPS integrated with the iSPI Performance for Quality Assurance.

— **FQDN**: specify the fully qualified domain name of the iSPI Performance for Metrics/NPS integrated with the iSPI Performance for Quality Assurance.

If you skip this integration and wish to enable this integration after installing the iSPI for IP Telephony, do as follows:

1. Open the nnm.extended.properties file present in the following directory: *nnmDataDir*`\shared\ipt\conf`
2. Change the values for the following properties as mentioned below:
   - `com.hp.ov.nms.spi.perfSPI.hostname=<host name for the machine that hosts the iSPI Performance for Metrics/NPS>`
   - `com.hp.ov.nms.spi.perfSPI.port=<port number for the machine that hosts the iSPI Performance for Metrics/NPS>`
   - `com.hp.ov.nms.spi.perfSPI.isPerfSPIIntegrated=true`
3. Restart the iSPI for IP Telephony using the following commands:
   a. **`ovstop -c iptjboss`**
   b. **`ovstart -c iptjboss`**
4. When the installation process is complete, click **Done**.

The iSPI for IP Telephony installer places the Avaya_IPT_CDR_Collection and the Cisco_IPT_CDR_Collection extension packs in the designated folder for NPS to process and deploy them

The iSPI for IP Telephony installation process is complete. You can check the necessary information about the installation from Summary and Details tab.

If the installation process fails to complete, you can rollback the installation process and start the installation again.

FTP Server Configuration

You must configure an FTP server on the management server. The `CDRonDemand` Web Service sends the CDR files from the Cisco Unified Communications Manager clusters to the iSPI for IP Telephony using this

FTP server. You must create at least one user on this FTP server and specify the credentials for the user in the iSPI for IP Telephony Configuration form when specifying the data access configuration.

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.

Starting the iSPI for IP Telephony

After installing the iSPI for IP Telephony on the NNMi management server, you must start the necessary processes.

Before starting the processes, you can check the status of NNMi with the following command:

```
ovstatus -c
```

Run the following command to start the necessary processes for the iSPI for IP Telephony:

```
ovstart -c iptjboss
```

If the above command fails to start the `iptjboss` process, follow these steps:

1. Run the following command to start all the processes required by NNMi and the iSPI for IP Telephony:

   ```
   ovstart -c
   ```

2. Check the status of the `iptjboss` process with the following command:

   ```
   ovstatus -c
   ```

You can stop the iSPI for IP Telephony processes with the following command:

```
ovstop -c iptjboss
```

Post Installation Configuration Tasks

Task 1: Use the iSPI for IP Telephony Configuration workspace to complete the following tasks for your IP Telephony environment:

- IP Phone exclusion filter configuration
- Data access configuration
- See the iSPI for IP Telephony Online Help > **Help for Administrators** for more information.

You can now see the IP Telephony nodes on NNMi.

Task 2: Seed the nodes that host the following IP Telephony Entities using the Discovery Configuration form in NNMi Configuration workspace if you have not seeded the nodes already:

- L2/L3 infrastructure devices such as switches and routers in your environment
- Avaya Communications Manager servers - 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) servers in your environment
- Avaya H248 Media Gateways - the G250s, G350s, G450s, and the G700s
- Cisco Unified Communications Manager (Call Manager) Servers in all the clusters in your environment
- Cisco Voice Gateways
- Cisco Gatekeepers
- Cisco SRSTs and Cisco Call Manager Express services
- Cisco Unity services
- Nortel Call Servers, Signaling Servers, and Media Gateways.

If the above mentioned nodes are already seeded, then you can wait for the next discovery of these nodes by NNMi to trigger a corresponding discovery of the iSPI for IP Telephony entities. Alternatively, if you have a small environment that you are managing, select these nodes from the NNMi node inventory and do a configuration poll for them.

See the *NNMi Online Help* for more information on seeding nodes and performing configuration polls for nodes.

Verifying the Installation

After installing the iSPI for IP Telephony, log on to the NNMi console with an administrative privilege, and then verify the availability of the following workspaces and views:

- **Cisco IP Telephony**

  In the Workspaces pane, click **Cisco IP Telephony**. Check if the names of the following views appear underneath:

  — Call Controllers

  — IP Phones

  — IC Trunks

  — Gatekeepers

  — Voice Gateways

  — Unity Devices

- **Nortel IP Telephony**

  In the Workspaces pane, click **Nortel IP Telephony**. Check if the names of the following views appear underneath:

  — Call Servers

  — Signaling Servers

  — IP Phones

  — Media Gateways

  — QOS Zones

- Avaya IP Telephony

  In the Workspaces pane, click **Avaya IP Telephony**. Check if the names of the following views appear underneath:

  — Call Controllers

— IP Phones

— Port Networks

— Media Gateways

Removing the iSPI for IP Telephony

To remove the iSPI for IP Telephony from a management server, follow these steps:

1. Log on to the management server with the `Administrator` (for Windows) or `root` (for UNIX) privileges.
2. Stop the iSPI for IP Telephony processes with the **`ovstop -c iptjboss`** command.
3. Run the following command at the command prompt:

   *On Windows: %NnmInstallDir%***`\uninstall\HPOvIPTiSPI\setup.exe`**

   *On UNIX: $NnmInstallDir***`/Uninstall/HPOvIPTiSPI/setup.bin`**

   A wizard opens.

   Alternatively, you can launch the wizard by inserting the iSPI for IP Telephony CD into the CD ROM, and then running the `setup.bat` or `setup` file (as applicable).
4. Follow the instructions on the wizard and complete the procedure to remove the iSPI for IP Telephony.
5. When the process is complete, click **Done**.

After uninstalling the iSPI for IP Telephony, you must uninstall the Cisco CDR IP Telephony and the Avaya CDR IP Telephony extension packs before re-installing the iSPI for IP Telephony.

After uninstalling the iSPI for IP Telephony, run the following commands to instruct `OvSPMD` to not consider the `iptjboss` process as a valid process:

- `ovstop -c`
- `ovstart -c`

License Information

The iSPI for IP Telephony includes a temporary Instant-On license key that is valid for 60 days after you install the iSPI for IP Telephony. You must obtain and install a permanent license key as soon as possible.

The three types of the iSPI for IP Telephony licenses are:

- Instant-on - The Instant-on license is an evaluation license. The valid period of this license is sixty days.
- 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.
- 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:
  - TA245AA HP NNM iSPI for IP Telephony 250 Phones Pack Migration SW LTU
  - TA246AA HP NNM iSPI for IP Telephony 1000 Phones Pack Migration SW LTU
  - TA247AA HP NNM iSPI for IP Telephony 5000 Phones Pack Migration SW LTU
  - TA256AA HP NNM iSPI for IP Telephony 250 Phones Pack Migration Non-production SW LTU
  - TA257AA HP NNM iSPI for IP Telephony 1000 Phones Pack Migration Non-production SW LTU
  - TA258AA HP NNM iSPI for IP Telephony 5000 Phones Pack Migration Non-production SW LTU

The 250 phone pack LTUs have a capacity of 1500 points, the 1000 phone pack LTUs have a capacity of 3000 points, and the 5000 phone pack LTUs have a capacity of 11,000 points.

The iSPI for IP Telephony consumes points from the common iSPI points license pool only when the consumption of the iSPI for IP Telephony is more than the total capacity of the migration licenses installed.

When the iSPI for IP Telephony consumes points from the common iSPI points license pool, it is equal to 1000 added to the difference between the consumption and the total capacity of the migration licenses installed.

To view the iSPI points consumed by the iSPI for IP Telephony, the total iSPI points consumed by all the Smart Plug-ins installed on the system, the installed capacity of the iSPI for IP Telephony migration licenses and the consumption of the migration licenses, do as follows:

a. In the NNMi console, click **Help > System Information**.

b. From the System Information box, click **View Licensing Information**.

Checking the License Type

To find the iSPI for IP Telephony license information, use any *one* of the following methods:

1. In the NNMi console, click **Help > About Network Node Manager i Software**.
2. In the About Network Node Manager window, click **Licensing Information**.

OR

1. In the NNMi console, click **Help > System Information**.
2. From the System Information box, click **View Licensing Information**.

Installing the iSPI for IP Telephony Migration Licenses:

After you purchase a migration license, install the license using one of the following methods:

- At the command prompt from the NNMi management server, use the following:
  - Windows: *%NnmInstallDir%*`\bin\nnmlicense.ovpl <IPTSPI> -f` <license_file>
  - UNIX: `opt/OV/bin/nnmlicense.ovpl <IPTSPI> -f <license_file>`
- From the AutoPass user interface, use the following:
  - Windows:
    - *%NnmInstallDir%*`\bin\nnmlicense.ovpl IPTSPI -gui`

- — *%NnmInstallDir%*\bin\nnmlicense.ovpl IPTSPI -g
- — UNIX:
  - – opt/OV/bin/nnmlicense.ovpl IPTSPI -gui
  - – opt/OV/bin/nnmlicense.ovpl IPTSPI -g

After you install your license from Autopass user interface, close the license window. The license points appear in the iSPI for IP Telephony system information only after you close the window.

Installing the iSPI Points Licenses

After you obtain iSPI Points licenses, install the licenses as mentioned in the HP NNMi documentation.

Obtaining the iSPI for IP Telephony Migration Licenses or iSPI Points Licenses

To extend the licensed capacity, purchase and install an additional iSPI for IP Telephony migration or iSPI Points License, contact your HP Sales Representative or your Authorized Hewlett-Packard Reseller for information about the iSPI for IP Telephony licensing structure, and to learn how to add license tiers for enterprise installations.

To obtain additional license keys, go to the HP License Key Delivery Service:

https://webware.hp.com/welcome.asp

Updating the Security Mode (HTTP to HTTPS)

After installing NNMi and iSPI for IP Telephony, if you want to modify the security mode from HTTPS or HTTP or from HTTP to HTTPS without installing the NNMi and iSPI for IP Telephony again, follow these steps:

1. On the management server, open the `nnm.extended.properties file` from the *nnmDataDir*`\shared\ipt\conf` or *$NnmdataDir*/`shared/ipt/conf` directory (depending on the type of the management server) with a text editor.
2. Update the values to true or false from the following:

- `com.hp.ov.nms.spi.ipt.Nnm.isSecure=false`: To modify the mode of communication used by iSPI for IP Telephony to communicate with NNMi.
- `com.hp.ov.nms.spi.ipt.spi.isSecure=false`: To modify the mode of communication used by NNMi to communicate with the iSPI for IP Telephony.

The value true represents HTTPS mode of communication and the value false represents HTTP mode of communication.

Always select the same mode of transmission for NNMi and iSPI for IP Telephony.

3 Restart the iSPI for IP Telephony with the following commands:

a **ovstop -c iptjboss**

b **ovstart -c iptjboss**

Configuring iSPI for IP Telephony to Use Modified NNMi Ports

After installing the iSPI for IP Telephony, you can modify the following configuration parameters: NNMi HTTP port, HTTPS port, and JNDI port

You can configure the iSPI for IP Telephony to use the modified NNMi ports by following the steps listed:

1 Open the `NnmDataDir/conf/nnm/props/nms-local.properties` file.

2 Obtain the values of the following properties: `jboss.http.port`, `jboss.https.port`

3 Replace the value for `-Djboss.nnm.port` property with the value of the jboss.http.port obtained in the previous step in the `nms-ipt.ports.properties` file present in the *nnmDataDir*`\shared\ipt\conf` directory.

4 Replace the value for `com.hp.ov.nms.spi.ipt.Nnm.port` property with the value of the jboss.http.port obtained in the previous step in the `nnm.extended.properties` file present in the *nnmDataDir*`\shared\ipt\conf` directory.

5 Replace the value for `com.hp.ov.nms.spi.ipt.Nnm.secureport` property with the value of the jboss.https.port obtained in the previous step in the `nnm.extended.properties` file present in the *nnmDataDir*`\shared\ipt\conf` directory.

6 Restart the iSPI for IP Telephony with the following commands:

   a **`ovstop -c iptjboss`**

   b **`ovstart -c iptjboss`**

Configuring iSPI for IP Telephony to Use Modified NNMi Web Services Client User Name and or Password

If you have changed the password for the NNMi Web Services client user specified during the installation of the iSPI for IP Telephony, do as follows:

1 Log on to the NNMi management server.

2 Run the following commands:

   a **`encryptiptpasswd.ovpl -e ipt`** *<new_password>*

   b **`encryptiptpasswd.ovpl -c ipt`**

3 Restart the iSPI for IP Telephony with the following commands:

   a **`ovstop -c iptjboss`**

   b **`ovstart -c iptjboss`**

If you want to configure the iSPI for IP Telephony to use an NNMi Web Service Client user name that is different from the user name specified during the installation of the iSPI for IP Telephony, do as follows:

1 Edit the `nnmDataDir/shared/ipt/conf/nnm.extended.properties` file and change the value of the following property: `com.hp.ov.nms.spi.ipt.Nnm.username`

2 Run the following commands:

   a **`encryptiptpasswd.ovpl -e ipt`** *<password for the new user>*

   b **`encryptiptpasswd.ovpl -c ipt`**

3 Restart the iSPI for IP Telephony with the following commands:

a **ovstop -c iptjboss**

b **ovstart -c iptjboss**

Modifying iSPI for IP Telephony Ports

The iSPI for IP Telephony jboss application server uses the following default ports unless you have modified them during the installation of the iSPI for IP Telephony:

- -Djboss.http.port=10080
- -Djboss.jnp.port=10099
- -Djboss.https.port=10443
- -Djboss.rmi.port=10083
- -Djboss.jrmp.port=10084
- -Djboss.pooled.port=10085
- -Djboss.socket.port=10086
- -Djboss.bisocket.port=10087
- -Djboss.ws.port=10088
- -Djboss.ejb3.port=10089
- -Djboss.nnm.port=80
- -Djboss.jmsControl.port=10458
- -Djboss.ssljmsControl.port=10091
- -Djboss.sslbisocket.port=10092

If you want to modify the HTTP or HTTPS ports for the iSPI for IP Telephony jboss application server, do as follows:

1 Replace the value for `-Djboss.http.port and -Djboss.https.port` properties with the new values in the `nms-ipt.ports.properties` file present in the *nnmDataDir*`\shared\ipt\conf` directory.

2 Replace the value for `com.hp.ov.nms.spi.ipt.spi.port` property and the `com.hp.ov.nms.spi.ipt.spi.secureport` property with the new values in the `nnm.extended.properties` file present in the *nnmDataDir*`\shared\ipt\conf` directory.

3 Restart the iSPI for IP Telephony with the following commands:

   a **`ovstop -c iptjboss`**

   b **`ovstart -c iptjboss`**

Accessing Installation Log Files

NNMi stores all the installation-related information into the following directory:

- **On Windows:**

  <*DRIVE*>:`\Documents and Settings\Administrator\Local Settings\Temp`

- **On UNIX:**

  `/tmp/`

4 Installing in a High-Availability Cluster or an Application Fail-over Environment

If you are installing the iSPI for IP Telephony in an application fail-over environment, you must install the iSPI for IP Telephony on both the primary and secondary NNMi management servers. See the *HP NNM i Software Smart Plug-in for IP Telephony Deployment Guide* for more details.

You can install NNMi in a high-availability (HA) or application fail-over environment to achieve redundancy in your monitoring setup. You can install the iSPI product in an HA environment where NNMi has been installed.

Prerequisites

Before you begin the installation for the HA environment, read the *Configuring HP NNM i Software in a High Availability Cluster* in the *NNMi Deployment and Migration Guide* to understand the NNMi HA configuration.

Make sure to meet the following requirements before installing iSPI for IP Telephony in an HA environment:

- The iSPI for IP Telephony runs on the NNMi management server.
- The iSPI for IP Telephony uses the same embedded database instance as NNMi.

Installing the iSPI in an HA Environment

If NNMi is not installed in an HA environment, install NNMi and the iSPI for IP Telephony together.

To install the iSPI for IP Telephony when NNMi is Running in the HA environment, follow these steps:

1. If NNMi is already configured and running in HA environment, unconfigure NNMi.
2. Start the iSPI installation.
3. After installation, configure NNMi and iSPI in the HA environment.

Configuring and Unconfiguring the iSPI in the HA Environment

Use the following commands to configure iSPI for IP Telephony:

- *Windows:*

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

- *UNIX:*

  *$NnmInstallDir***/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon IPT**

Use the following commands to unconfigure the iSPI:

- *Windows:*

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

- *UNIX:*

  *$NnmInstallDir***/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon IPT**

Removing the iSPI in an HA Environment

To remove the iSPI, follow these steps:

1. If NNMi is already configured and running in the HA environment, unconfigure the iSPI for IP Telephony.
2. Unconfigure NNMi in the HA environment.
3. Uninstall the iSPI for IP Telephony.
4. Configure NNMi in the HA environment.

For steps to unconfigure NNMi, see *Configuring HP NNM i Software in a High Availability Cluster* in the *NNMi Deployment and Migration Guide*.

You must install valid iSPI for IP Telephony licenses or common iSPI points licenses on both the physical servers in your HA setup. For more information about deploying the iSPI for IP Telephony in an HA environment, see the *HP NNM i Software Smart Plug-in for IP Telephony Deployment Guide*.

5 Getting Started with the iSPI for IP Telephony

After you complete the installation of the iSPI for IP Telephony in your NNMi environment, you can start monitoring your IP telephony network with the combination of NNMi and iSPI for IP Telephony. After installation, the iSPI for IP Telephony starts automatically discovering the IP telephony network and all the associated devices with an interval of one day.

Accessing the iSPI for IP Telephony

To access the details collected by the iSPI for IP Telephony after the initiation of the first discovery polling cycle, follow these steps:

1. Launch the NNMi console.
2. Log on to the NNMi console with one of the following user roles:
   - Administrator
   - Operator level 1
   - Operator level 2
   - Guest
3. In the Workspace pane, click **Cisco IP Telephony**, **Avaya IP Telephony**, or **Nortel IP Telephony** (depending on the type of network you want to monitor), and then click individual views to see details on the discovered network and devices.

Accessing the Online Help

To see the details presented by individual views and forms that are introduced by the iSPI for IP Telephony, you can refer to the *iSPI for IP Telephony Online Help*.

To launch the *iSPI for IP Telephony Online Help*, click **Help > Help for NNM iSPIs > IP Telephony Online Help**.

You can use the table of contents of the online help to navigate through different topics of the iSPI for IP Telephony online help. To open the table of contents for the online help, click **iSPI for IP Telephony** in the left pane of the online help.

A Troubleshooting

Linux Platform-related Troubleshooting Guidelines

If you are managing IPv4 IP Telephony nodes through IPv6 address management, using the iSPI for IP Telephony in a Linux environment, you must do as follows:

Modify the `run.sh` present in the following directory: /opt/OV/nonOV/ipt/jboss/bin/ file as follows:

1. Stop the IPT processes by using the command: **`ovstop -c iptjboss`**
2. From the `/opt/OV/nonOV/ipt/jboss/bin/` location, open the `run.sh` file.
3. Update the following line and change the value of `Djava.net.preferIPv4Stack=true` to `Djava.net.preferIPv4Stack=false`.
4. Restart the IPT jboss processes by using the command: **`ovstart -c iptboss`**

Starting the iSPI for IP Telephony

- The ovstart process stops responding and fails to start the iptjboss process after you install the iSPI for IP Telephony. You might get the following error messages when you use the `ovstart -c` and the `ovstatus -c` commands:

  ```
  ovstart -c

  iptjboss - FAILED Unable to start process using start command.

  ovspmd: Attempt to start HP OpenView services is complete.
  ```

```
ovstatus -c

ovspmd: Could not successfully run the status command
(nmsiptstatus.ovpl) for process iptjboss

iptjboss - FAILED The LRF-specified status command failed.
```

Workaround: This problem might occur if there is a conflict in the port numbers. You can perform the following steps to resolve this problem:

1. Make sure that you have installed all the necessary patches for NNMi. See the NNMi Installation Guide for more information.
2. Verify the jbossServer.log file present in the ipt log folder present at the following location: `nnmDataDir/log/ipt` for any entry specified as `ROOT CAUSE` in the deployment of Java MBeans. If there are any port conflicts, you can edit the values in the `nms-ipt.ports.properties` file present under the following directory: `nnmDataDir\shared\ipt\conf`
3. Check the `iptjboss` startup process by running the nmsiptstart.ovpl script present under the following directory: `%NNMInstallDir%\bin`.
4. Verify the `spiOvspmd.log` file in the ipt log folder. This file includes the results of the twiddle commands that invoke the iptjboss process. This file lists the connection exceptions (`ConnectionExceptions`) at the beginning of the process and displays the messages at the end of the file indicating that the process is started.

If the listed steps do not resolve the problem, you might have to uninstall and re-install the iSPI for IP Telephony

- After starting the iptjboss process, the process displays its status as `RUNNING` even after the process has failed to start.

Workaround: This problem might occur if the `iptjboss` fails to start due to installation issues, port conflicts, or authentication issues. You can perform the following steps to resolve this problem:

1. Check if the `iptjboss` process is running as follows:
   - Using the `ps` command on HP-UX, Solaris, or Linux operating systems
   - Using the **Task Manager** on Microsoft Windows operating systems
2. Use the `nmsiptstart.ovpl` , `nmsiptstatus.ovpl` , and `nmsiptstop.ovpl` scripts present in the `NNM_BIN` directory to verify the problem

3 Verify the jbossServer.log file present at the following locationnnmDataDir\log\ipt for any entry specified as ROOT CAUSE in the deployment of Java MBeans. Also, make sure that there are no port-related exceptions in the log file.

4 Verify the spiOvspmd.log file present in the ipt log folder for any authentication problem logged while running the twiddle commands to start the iptjboss process. If you see any error messages in the log file from the following scripts: nmsiptstart.ovpl, nmsiptstop.ovpl, or nmsiptstatus.ovpl for issues related to authentication or port numbers, you must update the proper user name and password using the encryptiptpassword.ovpl script and update the port numbers in the nms-ipt.ports.properties file and the nnm.extended.properties file present in the nnmDataDir\shared\conf\ipt directory.

- The iptjboss process stops responding to the OVsPMD commands (ovstart, ovstop, and ovstatus) when the system resource usage is high. The process stops responding to further OVsPMD commands and the process state changes to FAILED

Workaround: This problem might occur due to a failure by the twiddle commands to invoke the iptjboss process due to the high system resource usage. You can resolve this problem as follows:

1 Stop the iptjboss process using the nmsiptstop.ovpl command and check for the shutdown complete message for the process in the jBossServer.log file to see if the process is stopped.

2 If you did not find the shutdown complete message for the process in the previous step, run the nmsipthalt.ovpl script to halt the iptjboss process. Verify the jBossServer.log file to make sure that no instances of the process is still running. You can also check the Task Manager (for Microsoft Windows operating systems) and use the ps command on the HP-UX, Solaris, or Linux operating systems to verify that there are no instances of the iptjboss process running.

3 If you are unable to stop the iptjboss process with the steps listed, you can end the process as follows and then perform the step to start the process:

   a End the process from the Task Manager for Microsoft Windows operating systems

   b Kill the process using the kill <process_id> where <process_id> is the process ID of the Java instance for the iptjboss process.

c. Run the `nmsiptstart.ovpl` script to start the `iptjboss` process

d. Run the `ovstatus -c` command to confirm that the `OVsPMD` commands now use the current status of the iptjboss process

- Multiple instances of the iptjboss process result in the iptjboss process not working as expected.

Workaround: This problem might occur when you restart all the processes including the NNMi processes after you encounter a `FAILED` state for the `iptjboss` process. The `ovstop` command does not stop the underlying Java processes when you execute this command after encountering a `FAILED` state for the `iptjboss` process. The `ovstart` command executed, creates another instance of the `iptjboss` process, thus resulting in multiple `iptjboss` processes. This causes port conflicts and the `iptjboss` process does not work as expected. You can resolve this problem as follows:

1. Stop the `iptjboss` process using the `nmsiptstop.ovpl` command and check for the shutdown complete message for the process in the `jBossServer.log` file to see if the process is stopped.
2. If you did not find the shutdown complete message for the process in the previous step, run the `nmsipthalt.ovpl` script to halt the `iptjboss` process. Verify the `jBossServer.log` file to make sure that no instances of the process is still running. You can also check the `Task Manager` (for Microsoft Windows operating systems) and use the `ps` command on the HP-UX, Solaris, or Linux operating systems to verify that there are no instances of the `iptjboss` process running.
3. If you are unable to stop the `iptjboss` process with the steps listed, you can end the process as follows and then perform the step to start the process:

   a. End the process from the `Task Manager` for Microsoft Windows operating systems

   b. Kill the process using the `kill <process_id>` where `<process_id>` is the process ID of the Java instance for the `iptjboss` process.

   c. Run the `nmsiptstart.ovpl` script to start the `iptjboss` process

   d. Run the `ovstatus -c` command to confirm that the `OVsPMD` commands now use the current status of the iptjboss process

- *Problem:* The iSPI for IP Telephony installation stops abruptly.

  Solution: Check the error messages and available disk space; check if you have necessary permissions on the management server.

Removing the iSPI for IP Telephony

- *Problem:* The uninstallation process starts but does not end.

  Solution: Make sure that all the NNMi processes are running, stop the `iptjboss` process with the **`ovstop -c iptjboss`** command, and then try to remove the iSPI with the uninstallation wizard.

- *Problem:* After removing the iSPI for IP Telephony, the status of `iptjboss` appears as FAILED.

  Solution: Run the following commands in the given sequence:

  — **`ovstop -c`**

  — **`ovstart -c`**

  If you check the status again, `iptjboss` does not appear.

Index

W