HP Network Node Manager iSPI for IP Telephony Software

for the Windows® operating system

Software Version: 9.20

Installation Guide

Document Release Date: June 2013
Software Release Date: May 2012

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notices

Trademark Notices

Oracle Technology — Notice of Restricted Rights

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/).

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 Introduction

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

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

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

The NNM 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 NNM 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 NNM 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 NNM iSPI for IP Telephony supports Cisco, Avaya, Microsoft, and Nortel IP Telephony networks.

IP Telephony Workspaces

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

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

2 Before You Begin

Before you start installing the NNM 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 9.20 Installation Guide*
- *HP Network Node Manager i Software 9.20 Deployment Reference*
- *HP Network Node Manager i Software 9.20 Release Notes*
- *HP Network Node Manager i Software 9.20 Support Matrix*
- *HP Network Node Manager iSPI Performance for Metrics Software/NPS 9.20 Installation Guide*
- *HP Network Node Manager iSPI Performance for Metrics Software/NPS 9.20 Support Matrix*
- *HP Network Node Manager iSPI Performance for Metrics Software/NPS 9.20 Release Notes*

Before you begin, make sure that NNMi is installed in the environment and running. You must install the NNM 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 NNM 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.

Note Down the Details of the Oracle Server

Skip this task if you choose to use the embedded database with NNMi.

Note down the following details of the Oracle database instance that you want to use with the NNM iSPI.

- Port: The port used by the Oracle database.
- Hostname: Note down the fully-qualified domain name of the database server.
- Database name: Name of the Oracle database instance created for the Leaf Collector.
- User name: The Oracle user name created to access the above instance.
- Password: Password of the above user.

With the NNM 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 9.20 is installed and running on the machine where you plan to install the NNM iSPI for IP Telephony.

NNM iSPI Performance for Metrics/NPS

If you want to view reports with the data collected by the NNM iSPI for IP Telephony, you must make sure that the NNM iSPI Performance for Metrics/NPS 9.20 is running in the environment.

Check System Requirements

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

Refer to the *HP Network Node Manager iSPI for IP Telephony Software Support Matrix* and *HP Network Node Manager iSPI for IP Telephony Software Release Notes* documents for comprehensive details 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 iSPI for IP Telephony Software Support Matrix*	
Operating system	*HP Network Node Manager iSPI for IP Telephony Software Support Matrix*	
Database	*HP Network Node Manager iSPI for IP Telephony Software Support Matrix*	
Browser	*HP Network Node Manager iSPI for IP Telephony Software 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. If you want to install multiple iSPIs on the management server, create one Web Service Client user for each iSPI.

Do not use the NNMi **system** account while installing the NNM 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 NNM iSPI for IP Telephony. While installing and configuring the NNM iSPI for IP Telephony, do not use the same Oracle instance that was configured with NNMi.

Task 3: *Only for the Avaya IP Telephony.* Enable SNMPv1 and SNMPv2c

- Both SNMPv1 and SNMPv2c must be enabled on Avaya Communication Managers and Avaya Local Survivable Processors (LSPs).
- On every Avaya Communication Manager and Avaya LSP, make sure that community strings specified for SNMPv1 and SNMPv2c agents are identical.

Task 4: Tasks for Monitoring the Microsoft Lync Server Environment

Skip this task if you do not want to monitor the Microsoft Lync Server environment.

If you want to monitor the Microsoft Lync Server environment, you must perform the following tasks:

1. Install Microsoft .NET 3.5 or higher on the NNMi management server.

   Microsoft .NET Framework uses the port 80; therefore, you cannot use the default NNMi HTTP port. If you configured NNMi to use a non-default HTTP port, you can install .NET Framework 3.5 (or higher) any time before installing the NNM iSPI for IP Telephony.

   If you installed NNMi with the default HTTP port configuration on a system where .NET Framework 3.5 (or higher) is not installed, follow these steps to configure NNMi to use a non-default HTTP port:

   a. Log on to the NNMi management server.

   b. Go to the following directory:

      `%nnmdatadir%\conf\nnm\props`

   c. Open the `nms-local.properties` file with a text editor.

   d. Change the value of the property `jboss.http.port` to a non-default value. The default port is `80`. Set the property to a port that is available for use on the system.

   e. Save the `nms-local.properties` file.

   f. Restart NNMi by running the following commands:

      – **`ovstop -c`**

      – **`ovstart -c`**

      You can now install .NET 3.5 on the system.

2. Make sure that Microsoft PowerShell 2.0 is installed on the NNMi management server.

3. Specify the Community Strings of Microsoft Lync Servers and Gateways.

You must specify the community strings of Microsoft Lync servers and gateways that you want to monitor in the Default Read Community String form; you can launch this form from the Communication Configuration menu in the Configurations workspace in the NNMi console. For more information, see the *NNMi Help for Administrators*.

Task 5: Configuration Tasks on NNMi

If you want to install the NNM iSPI for IP Telephony in a Network Address Translation (NAT) environment with overlapping or duplicate addresses domains, see the *NNM iSPI for IP Telephony Deployment Guide*.

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

- Automatic discovery rules: It is recommended that you set up the auto-discovery rules for discovery of non-SNMP nodes that host IP phones on 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 the NNM 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 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, each Avaya Control LAN, 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 NNM 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*.
- Configure NNMi to discover the nodes that host Cisco Voice Gateways, Cisco SRST routers, and Cisco Gatekeepers.
- Configure NNMi to discover the nodes that host Avaya LSPs.

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

To install the NNM iSPI for IP Telephony in a high-availability (HA) cluster or application environment, see the *NNM iSPI for IP Telephony Deployment Guide*.

3 Installing the NNM iSPI for IP Telephony

You can install the NNM iSPI for IP Telephony on the management server. You can use the installation wizard to install the iSPI. The installation wizard guides you through the installation process.

If you are updating the NNM iSPI for IP Telephony from earlier versions, see the *NNM iSPI for IP Telephony Deployment Guide* for upgrade instructions.

Installing on the Management Server

To install the NNM iSPI for IP Telephony on the management server, follow these steps:

1 Log on to the management server as `Administrator`.

2 Insert the iSPI installation CD into the CD-ROM drive.

3 If the installation wizard does not open automatically, double-click the `setup.exe` file in the root directory of the media.

The installation initialization process prompts you to choose the language you want to use. The installer configures your system for the installation and initializes the installation process.

4 On the Introduction (Install) page, review the overview information, and then click **Next**. The License Agreement page opens.

5 Review the End User License Agreement, select **I accept..**, and then click **Next**. The Select Features page opens.

6 Click **Next**.

7 Select one of the following options:

- If you want to use the embedded database, select Typical.
- If you want to use an Oracle database that runs on the standard port (1521), select Typical.
- If you want to use an Oracle database that runs on a non-standard port (other than 1521), select Custom.

8 **If you select Typical:**

Select Custom only if you want to use the Oracle database that uses a non-standard port. If you select Custom, go to step 9 on page 16.

g After selecting Typical, click **Next**. The Server Configuration page appears.

h In the Choose the Database Type section, select one of the following:

— HP Software Embedded Database

- Oracle

i Go to step j on page 16 if you selected the Oracle option.

If you selected HP Software Embedded Database, click **Next**. The Install Checks screen appears. The wizard checks for the available disk space. Go to step 9 on page 16.

j If you selected Oracle in the previous step, you must specify necessary details in the following screens:

- **Choose Database Initialization Type:** Select Primary Server Installation if you want to use a database that is not initialized. Select Secondary Server Installation if you want to use a database that is already initialized. After making the selection, click **Next**. The Enter Your Database Server Information screen appears.
- **Enter Your Database Server Information:** Type the hostname of the Oracle system and the database instance name, and then click **Next**. The Enter the Database User Account Information screen appears.
- **Enter the Database User Account Information:** Type the user name and password of the Oracle database instance, and then click **Next**. The Install Checks screen appears. The wizard checks for the available disk space.

9 **If you select Custom:**

If you selected Typical, go to step 10 on page 16.

a After selecting Custom, click **Next**. The Feature Selection page appears.

b Click **Next**. The Server Configuration page appears.

c In the Choose the Database Type section, select Oracle, and then click **Next**. The Choose Database Initialization Type screen appears.

d Select Primary Server Installation if you want to use a database that is not initialized. Select Secondary Server Installation if you want to use a database that is already initialized. After making the selection, click **Next**. The Enter Your Database Server Information screen appears.

e Type the hostname and port of the Oracle system and the database instance name, and then click **Next**. The Enter the Database User Account Information screen appears.

f Type the user name and password of the Oracle database instance, and then click **Next**. The Install Checks screen appears. The wizard checks for the available disk space.

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

11 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 NNM iSPI for IP Telephony and you did not manually remove the components that were already placed by the installer.

12 At one point, the IPT iSPI Configuration window opens.

13. In the IPT iSPI Configuration window, specify the following details:

NNMi Server: Information Required by IPT iSPI	IPT iSPI Server: Information Required by NNMi
NNMi FQDN: Type the fully qualified domain name of the NNMi management server.	IPT iSPI FQDN: Fully qualified domain name of the NNMi management server.
Web Service Client User Name: Name of the NNMi Web Service client user that you created.	IPT iSPI HTTP Port: Type the port number that will be used by the NNM iSPI for IP Telephony for the HTTP communication (default: 10080).
Web Service Client Password: Password of the above user	IPT iSPI HTTPS Port: Type the port number that will be used by the NNM iSPI for IP Telephony for the HTTPS communication (default: 10443).
Retype Password: Password of the above user	IPT iSPI JNDI Port: Type the port number that will be used by the NNM iSPI for IP Telephony as the JNDI port (default: 10099).

   The NNM iSPI for IP Telephony installer automatically detects the following values for NNMi: HTTP port, HTTPS port, and JNDI port.

14. Select the `isSecure` option in both the sections (NNMi Server: Information Required by IPT iSPI and IPT iSPI Server: Information Required by NNMi) if you have configured NNMi to use the HTTPS mode of communication. Selecting this option ensures that NNMi and the NNM iSPI for IP Telephony always use the secure mode of communication (HTTPS).

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

15. Click **OK**.
16. After the installation is complete, a message appears to inform you that the installation process is complete and you can manually start the NNM iSPI for IP Telephony processes. Click **OK**.
17. You can click the `Summary` tab to check if the installation is successful and you can click the `Details` tab to verify if the NNM iSPI for IP Telephony packages are successfully installed. You can click on the `View log` file link in the window to check the log details and errors, if any.
18. Click **Done**.

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

After completing the installation, the installer prompts you to create a proxy service. You must create a proxy service before accessing the Microsoft IP Telephony inventory. See the section Creating the Proxy Service on page 18 for instructions to create the proxy service. The NNM iSPI for IP Telephony installation process is complete. You can check the necessary information about the installation from Summary and Details tab.

The NNM 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. You can verify the log files present in the `%temp%` directory to identify any problems that might have occurred which caused an unsuccessful installation.

The `%temp%` directory on the system includes the following log files for the NNM iSPI for IP Telephony installation:

- `preInstall_ipt.log`
- `postInstall_ipt.log`
- *For Upgrade*. `ipt-preupgrade.log`

Creating the Proxy Service

You must use this procedure if you want to manage the Microsoft Lync Server infrastructure. If you do not want to manage the Microsoft Lync Server infrastructure, skip this procedure.

You must make sure that you have installed the following prerequisites before creating the proxy service:

- .NET Framework 3.5 or higher versions
- Microsoft Windows PowerShell 2.0 or higher versions

For Microsoft Windows 2008 platforms, the prerequisites listed are installed by default. You must enable the .NET Framework if it is not enabled. Follow the instructions in the section Enabling the .NET Framework on page 19 to enable .NET Framework in your system.

1 Make sure the port 8000 is available for use on the system.

   If the port 8000 is not available, follow these steps:

   a Go to the directory `%nnmdatadir%\shared\ipt\conf`.

   b Open the `msipt.proxy.properties` file with a text editor.

   c Set the `Port` property to an available port on the system.

   d Save the file.

2 Run the `createProxyService.ovpl` script present at the following location: `%nnminstalldir%\bin`. This opens the command prompt.

3 Type **Y** to run the script. This opens the Set Service Login dialog box.

4 Type the required log on credentials in the following boxes:

   — **Username:** Specify the user name in the following format: *domain name*\user name.

   The user must be able to run remote cmdlets on the Front End pools that will be seeded by NNMi. The user must also have the read access to the Lync Monitoring server database.

   — **Password:** Specify the password for the above user name

   — **Confirm Password:** Retype the password

5 Click **OK**. This creates the proxy service.

Changing the Port of the Proxy Service

To change the port of the proxy service that you created, follow these steps:

1. Go to the directory `%nnminstalldir%\bin`, and then run the `UninstallProxy.bat` script. The script removes the proxy service.
2. Go to the directory `%nnmdatadir%\shared\ipt\conf`.
3. Open the `msipt.proxy.properties` file with a text editor.
4. Set the `Port` property to an available port on the system.
5. Save the file.
6. Run the `createProxyService.ovpl` script available in the directory `%nnminstalldir%\bin`. The script installs the proxy service again on the system; the proxy service starts running with the port specified in step 4.

Changing the Credentials for the Proxy Service

If you want to change the credentials for the proxy service that you created, follow these steps:

1. Open the list of services running on the system. You can run **`services.msc`** from **Start** > **Run** to open the list of services.
2. Right-click **MSIPT Proxy** and select **Properties**
3. Specify the new credentials as required in the respective boxes.
4. Click **OK**.

> You must restart the proxy service to make the credential changes applicable.

Enabling the .NET Framework

1. Open the Server Manager on your system. You can do this by right-clicking on your system name and selecting **Manage** from the Windows Explorer.
2. Right-click **Features** and select **Add Features**. This opens the Add Features Wizard.
3. Select **.NET Framework**
4. Follow the steps prompted by the wizard to enable the .NET Framework.

This enables the .NET Framework on your system.

Starting the NNM iSPI for IP Telephony

After installing the NNM 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 NNM 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 NNM iSPI for IP Telephony:

```
ovstart -c
```

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

```
ovstatus -c
```

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

```
ovstop -c iptjboss
```

Post-Installation Configuration Tasks

After you install the NNM iSPI for IP Telephony, follow these steps:

1 Make sure that NNMi has discovered the nodes that host the following IP telephony elements:

- Cisco Voice Gateways, Cisco SRST routers, and Cisco Gatekeepers
- Avaya LSPs

2 Use the NNM iSPI for IP Telephony Configuration workspace to complete the following tasks for your IP Telephony environment:

- Configuration IP Phone exclusion filter
- *For Cisco IP Telephony.* Configure data access with AXL
  - Obtain the AXL credentials from to access Cisco Unified Communication Manager.
  - Configure the NNM iSPI for IP Telephony to access the Cisco Unified Communication Manager data with the help of the AXL API.

    See the *Configuring Data Access* topic in *NNM iSPI for IP Telephony Help for Administrators*.
- *For Cisco IP Telephony.* Configure data access with SSH
  - Obtain the SSH credentials to access Cisco Unified Communication Manager.
  - Configure the NNM iSPI for IP Telephony to access the Cisco Unified Communication Manager data with the help of the SSH protocol.

    See the *Configuring Data Access* topic in *NNM iSPI for IP Telephony Help for Administrators*.
- *For Avaya IP Telephony.* It is recommended that you configure the NNM iSPI for IP Telephony to access the Avaya System Access Terminal using the SSH protocol for scalable discovery and polling of IP addresses of Avaya IP phones. See the *Configuring Data Access* topic in *NNM iSPI for IP Telephony Help for Administrators* for more information.

For the Microsoft infrastructure

- Enable the periodic topology discovery
- Specify User exclusion filter

3 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:

- Avaya Communications Manager servers - each physical server in duplex redundant pairs of Primary Servers and each stand alone Primary Server that is not deployed in duplex redundant pairs
- Avaya H.248 Media Gateways - the G250s, G350s, G450s, and the G700s
- Cisco Unified Communications Manager servers in all the clusters in your environment
- Cisco Unified Communications Manager Express services
- Cisco Unity and Cisco Unity Connection
- Nortel Call Servers, Signaling Servers, and Media Gateways.

If the above nodes are already seeded, you can wait for the next discovery of these nodes by NNMi to trigger a corresponding discovery of the NNM 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.

4 Seed the L2/L3 infrastructure devices such as switches and routers in your environment.

5 Seed Microsoft Lync Server Front End Pools

In addition, you must also seed Microsoft Lync Server Front End pools if you want to monitor a Microsoft Lync Server environment. You must seed only one Front End pool for each Central Site. You can seed Front End pools by using the Add Frontend Communication Configuration page, which you can open from the NNM iSPI for IP Telephony Configuration Console.

For more information, see the *NNM iSPI for IP Telephony Help for Administrator*.

Verifying the Installation

After installing the NNM 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:

  — UCM Clusters

  — UCMEs

  — IP Phones

  — Gatekeepers

  — Unity Devices

  — Test Plan

  — Test Result Reports

- **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

- **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

  — Media Gateways

- **Microsoft IP Telephony**

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

  — Lync Sites

  — Servers

  — Gateways

  — Gateway Interfaces

  — Lync End Users

Removing the NNM iSPI for IP Telephony

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

1. Log on to the management server as `Administrator`.
2. Stop the NNM iSPI for IP Telephony processes with the **`ovstop -c iptjboss`** command.
3. Run the following command at the command prompt:

   %nnminstalldir%`\uninstall\HPOvIPTiSPI\setup.exe`

   A wizard opens.

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

➤ After uninstalling the NNM 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`

If you configured the NNM iSPI for IP Telephony to export CSV files for monitoring registered devices count, route list, and hunt list, you must manually delete the CSV files from the following directories:

- For registered devices count:
  `%nnmdatadir%\shared\ipt\CSVExport\Cisco\RegisteredDevicesCount`
- For route and hunt lists:
  `%nnmdatadir%\shared\ipt\CSVExport\Cisco\Configurations`

The `%temp%` directory on the system includes the following log files for the NNM iSPI for IP Telephony uninstallation:

- `preRemove_ipt.log`
- `postRemove_ipt.log`

Remove the Extension Packs

You must manually remove the extension packs for the NNM iSPI for IP Telephony from the NPS system. To remove the extension packs from the NPS system, follow these steps:

1. Log on to the NPS system with the root or administrator privileges.
2. Go to the following directory:

   On Windows

   <*NPS_Install_Dir*>`\NNMPerformanceSPI\bin`

   On Linux

   `/opt/OV/NNMPerformanceSPI/bin`
3. Run the following commands:
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_Call_Terms_Types`**
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_CDR_Collection`**
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_CMProcOccupancy_Sum`**
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_MGW_Calls`**
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_NWReg_DSP_CODEC_Sum`**
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_PN_Load_Stats`**
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_TG_Calls`**
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_TG_RP_Usage`**
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_Trunk_Activity`**
   - **`uninstallExtensionPack.ovpl -p Avaya_IPT_RTP_Session Metrics`**
   - **`uninstallExtensionPack.ovpl -p Cisco_IPT_Calls_By_Details`**
   - **`uninstallExtensionPack.ovpl -p Cisco_IPT_Calls_By_GWs`**

- **uninstallExtensionPack.ovpl -p Cisco_IPT_Calls_By_IP_Trunks**
- **uninstallExtensionPack.ovpl -p Cisco_IPT_Calls_Terminations_Type**
- **uninstallExtensionPack.ovpl -p Cisco_IPT_GW_BChannel_Activity**
- **uninstallExtensionPack.ovpl -p Cisco_IPT_GW_Call_Activity**
- **uninstallExtensionPack.ovpl -p Cisco_IPT_Media_Resources**
- **uninstallExtensionPack.ovpl -p Cisco_IPT_TFTP**
- **uninstallExtensionPack.ovpl -p Cisco_IPT_UCM_Call_Activity**
- **uninstallExtensionPack.ovpl -p Cisco_IPT_UCM_System_Health**
- **uninstallExtensionPack.ovpl -p Cisco_IPT_UCOS_Services**
- **uninstallExtensionPack.ovpl -p Cisco_IPT_VM_Systems**
- **uninstallExtensionPack.ovpl -p Microsoft_Exchange**
- **uninstallExtensionPack.ovpl -p Microsoft_Lync**
- **uninstallExtensionPack.ovpl -p Call_Reports**
- **uninstallExtensionPack.ovpl -p Gateway_Statistics**
- **uninstallExtensionPack.ovpl -p Gateway_BChannel_Activity**

Subsequent Installation of the NNM iSPI for IP Telephony with Different Ports

After removing the NNM iSPI for IP Telephony, if you want to install it again with different ports on the same system, follow these steps:

1. Before installing the iSPI for the second time, run the following commands:

   - **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplicationService ipt** *<nnmi_host_fqdn>* **http** *<iSPI_http_port>*
   - **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplicationService msipt** *<nnmi_host_fqdn>* **http** *<iSPI_http_port>*
   - **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplicationService ipt** *<nnmi_host_fqdn>* **http** *<iSPI_https_port>*
   - **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplicationService msipt** *<nnmi_host_fqdn>* **http** *<iSPI_https_port>*
   - **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplication ipt**

- **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplication msipt**

  In this instance:

  <username> is the system user for NNMi (the user account created during the NNMi installation)

  <password> is the password for the above user

  <nnmi_host_fqdn> is the fully qualified domain name of the NNMi management server specified during the NNMi installation

  <nnmi_jndi_port> is the JNDI port used by NNMi

  <iSPI_http_port> is the HTTP port used by the previous installation of the NNM iSPI for IP Telephony

  <iSPI_https_port> is the secure HTTP port used by the previous installation of the NNM iSPI for IP Telephony

2. Restart the `ovjboss` process by running the following commands:

   - **ovstop -c ovjboss**
   - **ovstart -c ovjboss**

3. Install and configure the NNM iSPI for IP Telephony to work with different ports.

4. Check that you are able to open the NNM iSPI for IP Telephony Configuration Console. If you are not able to open the NNM iSPI for IP Telephony Configuration Console, follow these steps:

   a. Run the following commands:

      — **nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService ipt** *<nnmi_host_fqdn>* **http** *<iSPI_http_port>*

      — **nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService ipt** *<nnmi_host_fqdn>* **http** *<iSPI_https_port>*

      — **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService ipt** *<nnmi_host_fqdn>* **http** *<iSPI_http_port>*

      — **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService msipt** *<nnmi_host_fqdn>* **http** *<iSPI_http_port>*

      — **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService ipt** *<nnmi_host_fqdn>* **http** *<iSPI_https_port>*

— **%nnminstalldir%\support\nnmtwiddle.ovpl -u** *<username>* **-p** *<password>* **-host** *<nnmi_host_fqdn>* **-port** *<nnmi_jndi_port>* **invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService msipt** *<nnmi_host_fqdn>* **http** *<iSPI_https_port>*

In this instance:

<username> is the system user for NNMi (the user account created during the NNMi installation)

<password> is the password for the above user

<nnmi_host_fqdn> is the fully qualified domain name of the NNMi management server specified during the NNMi installation

<nnmi_jndi_port> is the JNDI port used by NNMi

<iSPI_http_port> is the HTTP port used by the previous installation of the NNM iSPI for IP Telephony

<iSPI_https_port> is the secure HTTP port used by the previous installation of the NNM iSPI for IP Telephony

b Restart the `ovjboss` and `iptjboss` processes by running the following commands:

— **ovstop -c ovjboss**

— **ovstart -c iptjboss**

License Information

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:

- 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 NNM 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 NNM 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 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.

When the NNM 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 NNM iSPI for IP Telephony, the total iSPI points consumed by all the iSPIs installed on the system, the installed capacity of the NNM 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 NNM 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 NNM 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:

  `%nnminstalldir%\bin\nnmlicense.ovpl IPTSPI -f` *<license_file>*

- From the AutoPass user interface, use one of the following:
  - `%nnminstalldir%\bin\nnmlicense.ovpl IPTSPI -gui`
  - `%nnminstalldir%\bin\nnmlicense.ovpl IPTSPI -g`

After you install your license from Autopass user interface, close the license window. The license points appear in the NNM 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 NNM iSPI for IP Telephony Migration Licenses or iSPI Points Licenses

To extend the licensed capacity, purchase and install an additional NNM iSPI for IP Telephony migration or iSPI Points License, contact your HP Sales Representative or your Authorized Hewlett-Packard Reseller for information about the NNM 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 NNM iSPI for IP Telephony, if you want to modify the security mode from HTTPS to HTTP or from HTTP to HTTPS without installing the NNMi and NNM 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` directory 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 NNM iSPI for IP Telephony.

3. Restart the NNM iSPI for IP Telephony with the following commands:
   a. **`ovstop -c iptjboss`**
   b. **`ovstart -c iptjboss`**

Exporting Certificates from NPS Configured in SSL

When NNMi, NPS, and the NNM iSPI for IP Telephony are configured to use SSL, you must export the third-party Cognos certificate and add it to the trusted certificates list to ensure secure communication (using the HTTPS protocol) between the NPS and the NNM iSPI for IP Telephony server.

After installing the NNM iSPI for IP Telephony, if NPS is configured with SSL, follow these steps to export the Cognos certificates:

1. Export the third-party Cognos certificate
2. Add third-party Cognos certificate to the trusted certificates list

Exporting Cognos Certificate

To export the Cognos certificate using the browser keystone, follow these steps:

1 Log on to NPS directly, by pointing your browser at the following URL:

`https://`*<fully_qualified_domain_name>***:***<nps_https_port>*

In this instance, *<fully_qualified_domain_name>* is the fully qualified domain name of the NPS system and *<nps_https_port>* is the HTTPS port that NPS uses for secure communication. The default port that NPS uses for secure communication is 9305.

2 View the certificate and export it as a DER-encoded binary file. Name the file as "`npscert.cer`".

> Ignore any warning message that you may see.

3 Copy the exported certificate to a temporary location on the NNM iSPI for IP Telephony server.

Adding Cognos Certificate to the Trusted Certificates

After exporting the certificate, follow these steps to add the certificate in the trusted certificates list:

1 Stop the NNMi management server processes with the following command:

```
ovstop -c ovjboss
```

2 Run the following command to import the `npscert.cer` from the temporary location on the NNM iSPI for IP Telephony server into `nnm.truststore`:

```
%NnmInstallDir%\nonOV\jdk\nnm\jre\bin\keytool -importcert -keystore
%Nnmdatadir%\shared\nnm\certificates\nnm.truststore -file npscert.cer
-storepass ovpass -alias npscert
```

> Ignore any warning message that you may see.

3 Make sure that running the following command lists `npcert` as one of the entries:

```
%NnmInstallDir%\nonOV\jdk\nnm\jre\bin\keytool -list -keystore
%NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass
```

4 Start the NNMi management server processes with the following command:

```
ovstart -c
```

Configuring the NNM iSPI for IP Telephony to Use Modified NNMi Ports

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

You can configure the NNM 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:

- `nmsas.server.port.web.http`
- `nmsas.server.port.web.https`

3 Open the `nnm.extended.properties` file with a text editor from the `%nnmdatadir%\shared\ipt\conf` directory.

4 If you modified the NNMi HTTP port, replace the value for `com.hp.ov.nms.spi.ipt.Nnm.port` property with the value of the `nmsas.server.port.web.http` obtained in step 2.

5 If you modified the NNMi HTTPS port, replace the value for `com.hp.ov.nms.spi.ipt.Nnm.secureport` property with the value of the `nmsas.server.port.web.https` obtained in step 2.

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

   a **`ovstop -c iptjboss`**

   b **`ovstart -c iptjboss`**

Configuring the NNM 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 NNM 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 NNM iSPI for IP Telephony with the following commands:

   a **`ovstop -c iptjboss`**

   b **`ovstart -c iptjboss`**

If you want to configure the NNM 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 NNM 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 `iptjboss` process with the following commands:

   a **`ovstop -c iptjboss`**

   b **`ovstart -c iptjboss`**

Modifying NNM iSPI for IP Telephony Ports

The NNM iSPI for IP Telephony uses a set of ports for its operation. These ports are configured at the time of installation by the installer and the installer offers you the option to choose non-default values for the HTTP and HTTPS ports. The `server.properties` file (available under the `%nnmdatadir%\nmsas\ipt` directory) provides a list of those ports.

After installation, you can configure the NNM iSPI for IP Telephony to use different HTTP and HTTPS ports (different from what was configured at the time of installation).

If you want to modify the HTTP or HTTPS port of the NNM iSPI for IP Telephony, follow these steps:

1 Log on to the NNMi management server as administrator.

2 Run the following commands on the management server:

-
  ```
  %nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password>
  -host <nnmi_host_fqdn> -port <nnmi_jndi_port> invoke
  com.hp.ov.nms.topo:service=NetworkApplication
  setApplicationService ipt <nnmi_host_fqdn> http <iSPI_http_port>
  ```

-
  ```
  %nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password>
  -host <nnmi_host_fqdn> -port <nnmi_jndi_port> invoke
  com.hp.ov.nms.topo:service=NetworkApplication
  setApplicationService msipt <nnmi_host_fqdn> http <iSPI_http_port>
  ```

-
  ```
  %nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password>
  -host <nnmi_host_fqdn> -port <nnmi_jndi_port> invoke
  com.hp.ov.nms.topo:service=NetworkApplication
  setApplicationService ipt <nnmi_host_fqdn> https <iSPI_https_port>
  ```

-
  ```
  %nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password>
  -host <nnmi_host_fqdn>-port <nnmi_jndi_port> invoke
  com.hp.ov.nms.topo:service=NetworkApplication
  setApplicationService msipt <nnmi_host_fqdn> https <iSPI_https_port>
  ```

  In this instance:

  <username> is the system user for NNMi (the user account created during the NNMi installation)

  <password> is the password for the above user

  <nnmi_host_fqdn> is the fully qualified domain name of the NNMi management server specified during the NNMi installation

  <nnmi_jndi_port> is the JNDI port used by NNMi

  <iSPI_http_port> is the HTTP port used by the previous installation of the NNM iSPI for IP Telephony

  <iSPI_https_port> is the secure HTTP port used by the previous installation of the NNM iSPI for IP Telephony

3 Open the `server.properties` file with a text editor from the `%nnmdatadir%\nmsas\ipt` directory.

4 Replace the value of the `nmsas.server.port.web.https` property with the new HTTPS port.

5 Replace the value of the `nmsas.server.port.web.http` property with the new HTTP port.

6 Save the file

7 Restart the NNM iSPI for IP Telephony with the following commands:

   a **`ovstop -c ovjboss`**

   b **`ovstart -c iptjboss`**

Modifying the Embedded Database Port

If you configure the NNMi embedded database to use a port different from what was configured at the time of the installation of the NNM iSPI for IP Telephony, you must update the `server.properties` file with the new port number.

To update the `server.properties` file, follow these steps:

1 Log on to the NNMi management server as administrator.

2 Open the `server.properties` file with a text editor from the `%nnmdatadir%\nmsas\ipt` directory.

3 Replace the value of the `com.hp.ov.nms.postgres.port` property with the new embedded database port.

4 Save the file

5 Restart the `ovjboss` and `iptjboss` processes with the following commands:

   a **`ovstop -c iptjboss`**

   b **`ovstart -c iptjboss`**

Troubleshooting Tips

- *Problem:* The `ovstart` process stops responding and fails to start the iptjboss process after you install the NNM 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.
  ```

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

  a Make sure that you have installed all the necessary patches for NNMi. See the NNMi Installation Guide for more information.

b Verify the `boot.log` and `ipt-trace.log` files 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 `server.properties` file present under the following directory: `%nnmdatadir%\nmsas\ipt`

c Check the `iptjboss` startup process by running the `nmsiptstart.ovpl` script present under the following directory: `%nnminstalldir%\bin`.

d 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 NNM iSPI for IP Telephony

- *Problem:* NNM iSPI for IP Telephony forms (including the NNM iSPI for IP Telephony Configuration form) fail to open after you reinstall the NNM iSPI for IP Telephony and configure the reinstalled iSPI to work with ports different from the ones configured in the first installation.

  Solution: After reinstalling and configuring the iSPI to work with different ports, NNM iSPI for IP Telephony forms open with the old port setting, and as a result, connection error message appears in the browser.

  To resolve this, follow these steps:

  a Log on to the management server with the `administrator` privileges.

  b Run the following commands:

  –
  ```
  %nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p
  <password> -host <nnmi_host_fqdn> -port <nnmi_jndi_port> invoke
  com.hp.ov.nms.topo:service=NetworkApplication
  setApplicationService ipt <nnmi_host_fqdn> http <iSPI_http_port>
  ```

  –
  ```
  %nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p
  <password> -host <nnmi_host_fqdn> -port <nnmi_jndi_port> invoke
  com.hp.ov.nms.topo:service=NetworkApplication
  setApplicationService msipt <nnmi_host_fqdn> http <iSPI_http_port>
  ```

  –
  ```
  %nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p
  <password> -host <nnmi_host_fqdn> -port <nnmi_jndi_port> invoke
  com.hp.ov.nms.topo:service=NetworkApplication
  setApplicationService ipt <nnmi_host_fqdn> http <iSPI_https_port>
  ```

  –
  ```
  %nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p
  <password> -host <nnmi_host_fqdn>-port <nnmi_jndi_port> invoke
  com.hp.ov.nms.topo:service=NetworkApplication
  setApplicationService msipt <nnmi_host_fqdn> http <iSPI_https_port>
  ```

  In this instance:

  <username> is the system user for NNMi (the user account created during the NNMi installation)

  <password> is the password for the above user

  <nnmi_host_fqdn> is the fully qualified domain name of the NNMi management server specified during the NNMi installation

  <nnmi_jndi_port> is the JNDI port used by NNMi

<*iSPI_http_port*> is the HTTP port used by the NNM iSPI for IP Telephony

<*iSPI_https_port*> is the secure HTTP port used by the NNM iSPI for IP Telephony

c Restart the `ovjboss` and `iptjboss` processes by running the following commands:

- **`ovstop -c ovjboss`**
- **`ovstart -c iptjboss`**

4 Getting Started with the NNM iSPI for IP Telephony

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

Accessing the NNM iSPI for IP Telephony

To access the details collected by the NNM 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 NNM iSPI for IP Telephony, you can refer to the *NNM iSPI for IP Telephony Online Help*.

To launch the *NNM 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 NNM iSPI for IP Telephony online help. To open the table of contents for the online help, click **NNM iSPI for IP Telephony** in the left pane of the online help.

A Troubleshooting

Managing IPv4 IP Telephony Nodes Through IPv6 Address Management

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

Modify the `nms-ipt.jvm.properties` file present in the `%nnmdatadir%\shared\ipt\conf` directory as follows:

1. Stop the `iptjboss` processes by using the command: **`ovstop -c iptjboss`**
2. From the `%nnmdatadir%\shared\ipt\conf` directory, open the `nms-ipt.jvm.properties` file.
3. Change `Djava.net.preferIPv4Stack=true` to `Djava.net.preferIPv4Stack=false`.
4. Start the `iptjboss` processes by using the command: **`ovstart -c iptboss`**

Starting the NNM iSPI for IP Telephony

- The ovstart process stops responding and fails to start the iptjboss process after you install the NNM 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:

  a. Make sure that you have installed all the necessary patches for NNMi. See the NNMi Installation Guide for more information.

  b. Verify the `boot.log` and `ipt-trace.log` files present in the ipt log folder present at the `%nnmdatadir%\log\ipt` directory 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`.

c Check the iptjboss startup process by running the nmsiptstart.ovpl script present under the following directory: %nnminstalldir%\bin.

d 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 NNM 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:

  a Check that the iptjboss process is running.

  b Use the nmsiptstart.ovpl, nmsiptstatus.ovpl, and nmsiptstop.ovpl scripts present in the NNM_BIN directory to verify the problem

  c Verify the boot.log file present at the following location %nnmdatadir%\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.

  d 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. To resolve this problem, stop the iptjboss process using the nmsiptstop.ovpl command and check for the shutdown complete message for the process in the boot.log file to see if the process is stopped.

  If you are still not able to stop the iptjboss process, follow these steps:

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

  — Run the nmsiptstart.ovpl script to start the iptjboss process

  — 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. To resolve this problem, stop the `iptjboss` process using the `nmsiptstop.ovpl` command and check for the shutdown complete message for the process in the `boot.log` file to see if the process is stopped.

e. 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:

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

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

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

- The NNM 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.

- NNM iSPI for IP Telephony forms (including the NNM iSPI for IP Telephony Configuration form) fail to open after you reinstall the NNM iSPI for IP Telephony and configure the reinstalled iSPI to work with ports different from the ones configured in the first installation.

  Solution: After reinstalling and configuring the iSPI to work with different ports, NNM iSPI for IP Telephony forms open with the old port setting, and as a result, connection error message appears in the browser.

  To resolve this, follow these steps:

  a. Log on to the management server with the `root` privileges.

  b. Run the following commands:

     — **`%nnminstalldir%\support\nnmtwiddle.ovpl -u`** *<username>* **`-p`** *<password>* **`-host`** *<nnmi_host_fqdn>* **`-port`** *<nnmi_jndi_port>* **`invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService ipt`** *<nnmi_host_fqdn>* **`http`** *<iSPI_http_port>*

     — **`%nnminstalldir%\support\nnmtwiddle.ovpl -u`** *<username>* **`-p`** *<password>* **`-host`** *<nnmi_host_fqdn>* **`-port`** *<nnmi_jndi_port>* **`invoke com.hp.ov.nms.topo:service=NetworkApplication setApplicationService ipt`** *<nnmi_host_fqdn>* **`http`** *<iSPI_https_port>*

     In this instance:

     <username> is the system user for NNMi (the user account created during the NNMi installation)

     <password> is the password for the above user

     <nnmi_host_fqdn> is the fully qualified domain name of the NNMi management server specified during the NNMi installation

     <nnmi_jndi_port> is the JNDI port used by NNMi

     <iSPI_http_port> is the HTTP port used by the previous installation of the NNM iSPI for IP Telephony

     <iSPI_https_port> is the secure HTTP port used by the previous installation of the NNM iSPI for IP Telephony

  c. Restart the `ovjboss` and `iptjboss` processes by running the following commands:

- **`ovstop -c ovjboss`**
- **`ovstart -c iptjboss`**

Removing the NNM iSPI for IP Telephony

- 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.

- After removing the NNM 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.

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, 9.20

Document title: Installation Guide

Feedback: