HP Network Node Manager iSPI for IP Telephony Software

For the Windows ® operating system

Software Version: 10.00

Installation Guide

Document Release Date: July 2014

Software Release Date: July 2014

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

Oracle Technology — Notice of Restricted Rights

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

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

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: **http://www.hp.com/go/hpsoftwaresupport**

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services

- Enter into discussions with other software customers
- Research and register for software training

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

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

To find more information about access levels, go to:

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Contents 4
Chapter 1: Introduction 7
IP Telephony Workspaces 7
Related Documentation 8
Chapter 2: Before You Begin 9
Installation Plan on the NNMi Management Server 9
Preinstallation Tasks 10
Installing the NNM iSPI for IP Telephony in Microsoft Lync Server Environment 13
Installing MS IPT Proxy 15
Changing the Credentials Used for MS IPT Proxy 16
Enabling the .NET Framework 17
Changing the Port of the MS IPT Proxy 17
Installing in a High-Availability Cluster or an Application Fail-over Environment 18
Chapter 3: Installing the NNM iSPI for IP Telephony 19
Installing on the Management Server 19
Starting the NNM iSPI for IP Telephony 22
Post-Installation Configuration Tasks 23
Verifying the Installation 27
Integrating MS IPT Proxy with NNM iSPI for IP Telephony 29
Removing the NNM iSPI for IP Telephony 30
Remove the Extension Packs 31
Subsequent Installation of the NNM iSPI for IP Telephony with Different Ports 32
Updating the Security Mode (HTTP to HTTPS/HTTPS to HTTP) 33
Exporting Certificates from NPS (Configured to Use SSL) 34
Configuring the NNM iSPI for IP Telephony to Use the Modified NNMi Ports 35
Configuring the NNM iSPI for IP Telephony to Use the Modified NNMi Web Services Client User Name and Password 36
Modifying the NNM iSPI for IP Telephony Ports 37
Modifying the Embedded Database Port 37

Chapter 4: Getting Started with the NNM iSPI for IP Telephony 39
Accessing the NNM iSPI for IP Telephony 39
Accessing the Online Help 39
Chapter 5: Troubleshooting 41
Managing IPv4 IP Telephony Nodes Through IPv6 Address Management 41
Starting the NNM iSPI for IP Telephony 41
Removing the NNM iSPI for IP Telephony 44
We appreciate your feedback! 45

Chapter 1: Introduction

The HP Network Node Manager i Software Smart Plug-in for IP Telephony (NNM iSPI for IP Telephony) extends the capability of the 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 the 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 tsasks:

- Automatically discover the IP Telephony infrastructure
- Monitor the states related to fault and the usage of various discovered components of the IP telephony infrastructure
- Report on the call metrics (CDR data for Avaya, Cisco, Acme and Microsoft 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 the collection interval for the monitoring tasks, the various data access configurations, and the various thresholds for monitoring.

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

IP Telephony Workspaces

The NNM iSPI for IP Telephony introduces the following workspaces in the Workspaces pane in the NNMi console:

- **Cisco IP Telephony**
- **Avaya IP Telephony**
- **Acme IP Telephony**
- **Microsoft IP Telephony**
- **Nortel IP Telephony**

These workspaces enables you to view all the details indicating the health, performance, and availability of the Cisco, Avaya, Acme, Microsoft and Nortel IP Telephony network with the help of 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 the respective details forms.

Related Documentation

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

- **NNM iSPI for IP Telephony Online Help 10.00**—includes information on the views and forms introduced by the NNM iSPI for IP Telephony.
- **NNM iSPI for IP Telephony Release Notes 10.00**
- **NNM iSPI for IP Telephony Support Matrix 10.00**

Chapter 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 10.00 Interactive Installation Guide for Windows HP Network Node Manager i Software 10.00 Interactive Installation Guide for Linux*
- *HP Network Node Manager i Software 10.00 Deployment Reference*
- *HP Network Node Manager i Software 10.00 Release Notes*
- *HP Network Node Manager i Software 10.00 Support Matrix*
- *HP Network Node Manager i Software Smart Plug-in Performance for Metrics/NPS 10.00 Installation Guide*
- *HP Network Node Manager i Software Smart Plug-in Performance for Metrics/NPS 10.00 Support Matrix*
- *HP Network Node Manager i Software Smart Plug-in Performance for Metrics/NPS 10.00 Release Notes*

Before you begin, make sure that NNMi is installed in the environment and running. You can install the NNM iSPI for IP Telephony on the NNMi management server. You can also install the NNM iSPI for IP Telephony 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 as these details are required by the NNM iSPI for IP Telephony installer. The configuration-related details that you must note down are as follows:

- **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 for IP Telephony:

  - **Port:** The port used by the Oracle database.
  - **Hostname:** This is applicable when you use an Oracle database residing on a remote server. Note down the fully-qualified domain name (FQDN) of the database server.

- **Database name:** Name of the Oracle database instance.
- **User name:** The Oracle user name created to access NNMi data.
- **Password:** Password of the Oracle user name created to access NNMi data.

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 NNM iSPI for IP Telephony, see the *Database Installation* section in the*HP Network Node Manager i Software 10.00 Interactive Installation Guide for Windows* . If you are using a unique Oracle instance, note down the details, listed out in the previous paragraph, for this instance as well.

- **NNMi Installation**

Make sure that NNMi 10.00 is installed and is running on the machine where you plan to install the NNM iSPI for IP Telephony.

- **NNM iSPI Performance for Metrics/NPS**

Make sure that the NNM iSPI Performance for Metrics/NPS 10.00 is running if this application is a part of your deployment environment.

- **Check the System Requirements**

Make sure the managent server meets all the hardware and software requirements. For a complete information about the harware and software requirements and dependencies, see the *HP Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix 10.00*and the *HP Network Node Manager iSPI for IP Telephony Software Release Notes 10.00*.

The following table lists the preinstallation checklist for hardware and software requirements:

Requirement	Reference Document	Complete? (Yes/No)
Disk space	*HP Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix 10.00*	
Operating system	*HP Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix 10.00*	
Database	*HP Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix 10.00*	
Browser	*HP Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix 10.00*	

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 is used during the course of installation. If you want to install multiple iSPIs on the management server, you must create a Web Service Client user for each of the 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

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

Task 4: Monitor the Microsoft Lync Server Environment

To monitor the Microsoft Lync Server environment, perform the following tasks:

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

  The Microsoft .NET Framework uses port 80; therefore, you cannot use the default NNMi HTTP port. If you have 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. However, if you have installed the NNMi with the default HTTP port configuration on a system where .NET Framework 3.5 (or higher) is not installed, you must configure the NNMi to use a non-default HTTP port.

  To configure the NNMi to use a non-default HTTP port, follow these steps:

  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 `jboss.http.port` property 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 the NNMi by running the following commands:

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

You can now install the Microsoft .NET 3.5 on the system.

- Make sure that the Microsoft PowerShell 2.0 is installed on the NNMi management server.
- Specify the Community Strings of Microsoft Lync Servers and Gateways.

  You must specify the community strings of the 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 *HP Network Node Manager i Software Online Help: Help for Administrators 10.00*.

Task 5: Configuration Tasks on NNMi

> **Note:** For information about installing the NNM iSPI for IP Telephony in a Network Address Translation (NAT) environment with overlapping or duplicate addresses domains, see the *Overlapping IP Addresses* chapter of the *HP Network Node Manager iSPI for IP Telephony Software Deployment Reference 10.00*.

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

- Automatic discovery rules: It is recommended that you setup the auto-discovery rules for the discovery of non-SNMP nodes that host the 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 *HP Network Node Manager i Software Online Help: Help for Administrators 10.00*.
- 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, and the Cisco Call Manager Express nodes). Use the **Communication Configuration** form in the NNMi Configuration workspace to add these community strings in the list of default read community strings to be used by the 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 *HP Network Node Manager i Software Online Help: Help for Administrators 10.00*.
- Specify the communication configuration for the Avaya Communication Manager servers: It is recommended that the NNMi and the NNM iSPI for IP Telephony is configured to use either SNMP v1 or SNMP v3 for communication with the 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 the consistent behavior of the 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.You must complete this configuration task for all the Avaya Communications Manager server nodes, which includes the following:

- Each physical server in duplex redundant pairs of Primary Servers
- Each stand-alone Primary Server that is not deployed in duplex redundant pairs
- Each 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 the NNMi and the 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 about specifying Regions, see the *HP Network Node Manager i Software Online Help: Help for Administrators 10.00*.

- Configure NNMi to discover the nodes that host the Cisco Voice Gateways, Cisco SRST routers, and Cisco Gatekeepers.
- Configure NNMi to discover the nodes that host the Avaya LSPs.

Installing the NNM iSPI for IP Telephony in Microsoft Lync Server Environment

Unlike the other IP telephony environments, the Microsoft Lync Server environment does not support the discovery and monitoring of most of the IP telephony entities using the SNMP; only the gateways and Microsoft Lync servers require SNMP.

In Microsoft Lync Server environment, **MS IPT Proxy**, a .NET component, is responsible for most of the data collection using remote powershell commands. MS IPT Proxy acts as the communication interface between the NNM iSPI for IP Telephony and the Microsoft Lync server. All the requests (such as topology discovery, CDR collection, and so on) from the NNM iSPI for IP Telephony pass through MS IPT Proxy to the Microsoft Lync server. SNMP's role is limited to the discovery of gateways. In the absence of MS IPT Proxy, NNM iSPI for IP Telephony cannot discover or monitor Microsoft Lync Server environment.

You can install one or more proxies in your environment based on your requirements. However, you must always install the MS IPT Proxy only on a Windows server.

You can install the MS IPT Proxy either on the same Windows server that hosts the NNM iSPI for IP Telephony or on a different server.

To install the MS IPT Proxy and the NNM iSPI for IP Telephony on the same Windows server, follow these steps:

1. Install the Microsoft .NET 3.5 or higher on the Windows server where you plan to install the NNM iSPI for IP Telephonyand the MS IPT Proxy.

   The Microsoft .NET Framework uses port 80; therefore, you cannot use the default NNMi HTTP port. If you have 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. However, if you have installed the NNMi with the default HTTP port configuration on a system where .NET Framework 3.5 (or higher) is not installed, you must configure the NNMi to use a non-default HTTP port.

   To configure the NNMi to use a non-default HTTP port, follow these steps:

   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 `jboss.http.port` property 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 the NNMi by running the following commands:

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

   You can now install the Microsoft .NET 3.5 on the system.

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

3. Install the MS IPT Proxy on the Windows server. For more information, see Installing MS IPT Proxy.

4. Install the NNM iSPI for IP Telephony on the same Windows server. For more information, see Installing on the Management Server.

5. Integrate the MS IPT Proxy with the NNM iSPI for IP Telephony. For more information, see Integrating MS IPT Proxy with NNM iSPI for IP Telephony.

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

   You must specify the community strings of the 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 *HP Network Node Manager i Software Online Help: Help for Administrators 10.00*.

To install the MS IPT Proxy and the NNM iSPI for IP Telephony on the different Windows servers, follow these steps:

1. Install the Microsoft .NET 3.5 or higher on the Windows server where you plan to install the MS IPT Proxy.
2. Make sure that Microsoft PowerShell 2.0 is installed on the Windows server.
3. Install the MS IPT Proxy on the Windows server. For more information, see Installing MS IPT Proxy.
4. Install the NNM iSPI for IP Telephony on a different Windows server. For more information, see Installing on the Management Server.
5. Integrate the MS IPT Proxy with the NNM iSPI for IP Telephony. For more information, see Integrating MS IPT Proxy with NNM iSPI for IP Telephony.
6. Specify the Community Strings of Microsoft Lync Servers and Gateways.

   You must specify the community strings of the 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 *HP Network Node Manager i Software Online Help: Help for Administrators 10.00*.

Installing MS IPT Proxy

Before you start installing the MS IPT Proxy, make sure that the Windows server, where you plan to install the MS IPT Proxy, has the following frameworks installed on it:

- Microsoft .NET 3.5 or higher
- Microsoft PowerShell 2.0

Note: For Microsoft Windows 2008 platforms, the prerequisites listed in the previous paragraph are installed by default. However, you must enable the .NET Framework if it is not enabled. To enable the .NET Framework in your system, follow the instructions listed in Enabling the .NET Framework.

To install the MS IPT proxy, follow these steps:

1. Log on to the Windows server as `Administrator`.
2. Insert the NNM iSPI for IP Telephony installation CD into the CD-ROM drive.
3. In the `MS IPT Proxy` folder, double-click the `setup.exe` file in the root directory of the media.

The installation initialization process prompts you to choose the language that 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**.
6. On the **Choose the folders** page, accept the default location for the application and data folders, or browse to a different location.

   Note: This dialog box does not appear if you have installed other HP Software applications previously on this server.

7. Click **Next**. The **Install Checks** page opens. The wizard checks for the available disk space.
8. Click **Next**. The **Pre-Install Summary** screen appears. Review the options, and then click **Install**. The installation process begins.
9. During the process, when the MS IPT Proxy Credentials dialog box opens, type the required log on credentials in the boxes provided. The following table describes the boxes that appear in the dialog box:

Box Name	Description
Username	Type 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 are seeded by NNMi. The user must also have the `read` access to the Lync Monitoring server database.
Password	Type the password for the user.
Confirm Password	Retype the password.

10. Click **Done** to complete the installation.

Note: The MS IPT Proxy uses the port 8000 by default. If the port 8000 is not available on the system, you must change the port of the MS IPT Proxy. To change the port of MS IPT Proxy, see Changing the Port of the MS IPT Proxy.

Changing the Credentials Used for MS IPT Proxy

To change the credentials used for the MS IPT Proxy, follow these steps:

1. Open the list of services running on the system. (Execute `services.msc` from **Start** > **Run** to open the list of services.)
2. Right-click **MS IPT PROXY** and then select **Properties**.
3. Specify the new credentials in the respective boxes.
4. Click **OK**.

The changes made to the credentials become effective after the restart of the proxy service.

Enabling the .NET Framework

To enable the .NET framework, follow these steps:

1. Open the Server Manager on your system. (Right-click on your system name and then select **Manage** from the Windows Explorer.)
2. Right-click **Features** and then select **Add Features**. The **Add Features Wizard** opens.
3. Select **.NET Framework**, and then follow the steps prompted by the wizard to enable the .NET framework on your system.

Changing the Port of the MS IPT Proxy

To change the port of the MS IPT Proxy, follow these steps:

1. Open the list of services running on the system. (Execute `services.msc` from **Start** > **Run** to open the list of services.)
2. Right-click **MS IP PROXY** and then select **Stop**.
3. Go to the following directory:

   `%nnmdatadir%\shared\ipt\conf`
4. Open the `msipt.proxy.properties` file with a text editor.
5. Set the `Port` property to an available port on the system.

   Note: HP recommends that you do not change any values other than the port number of the properties available in the `msipt.proxy.properties` file.
6. Save the file.
7. Start the MS IPT Proxy.

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 an application fail-over environment, see the *HP Network Node Manager iSPI for IP Telephony Software Deployment Reference 10.00*.

Chapter 3: Installing the NNM iSPI for IP Telephony

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

Note: If you are upgrading the NNM iSPI for IP Telephony from earlier versions, follow the upgrade instructions. For more information about the upgrade instructions, see the *HP Network Node Manager iSPI for IP Telephony Software Upgrade Reference 10.00*.

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 NNM iSPI for IP Telephony installation CD into the CD-ROM drive.
3. Double-click the `setup.exe` file in the root directory of the media, if the installation wizard does not open automatically.

   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** screen appears.
5. Review the End User License Agreement, select **I accept..**, and then click **Next**. The **Select Features** page opens.
6. 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**.

   Typical

   If you select **Typical**, follow these steps:

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

b. In the **Choose the Database Type** section, select one of the following:

- **HP Software Embedded Database**: If you select this option, click **Next**. The **Install Checks** screen appears. The wizard checks for the available disk space. Go to Step 7.
- **Oracle**: If you select this option, click **Next**, and then specify the following details in the screens that follow:
  - **Choose Database Initialization Preferences**: To use a database that is not initialized, select **Primary Server Installation**, and to use a datasbase that is already initialized, select **Secondary Server Installation**. After selecting, 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. Go to Step 7.

Custom

If you select **Custom**, follow these steps:

a. 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. To use a database that is not initialized, select **Primary Server Installation**, and to use a datasbase that is already initialized, select **Secondary Server Installation**. After selecting, click **Next**. The **Enter Your Database Server Information** screen appears.

e. 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.

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.

g. Go to Step 7.

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

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

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

During the installation process, the NNM iSPI for IP Telephony Configuration window appears.

9. a. On the NNM iSPI for IP Telephony Configuration window, specify the following details:
    - **NNMi Server: Information Required by IPT iSPI** Section -
        - NNMi FQDN: Type the fully qualified domain name of the NNMi management server.
        - Web Service Client User Name: Type the name of the NNMi Web Service client user that you created.
        - Web Service Client Password: Type the password of the NNMi Web Service client user.
        - Retype Password: Retype the password of the the NNMi Web Service client user.
    - **IPT iSPI Server: Information Required by NNMi** Section -
        - IPT iSPI FQDN: Type the fully qualified domain name of the NNMi management server.
        - IPT iSPI HTTP Port: Type the port number to be used by the for the HTTP communication (default: 10080).
        - IPT iSPI HTTPS Port: Type the port number to be used by the for the HTTPS communication (default: 10443).
        - IPT iSPI JNDI Port: Type the port number to be used by the as the JNDI port (default: 10099).

    Note: The NNM iSPI for IP Telephony installer automatically detects the following values for NNMi:
    - HTTP port
    - HTTPS port
    - JNDI port

    b. If you have configured NNMi to use the HTTPS mode of communication, select the `isSecure` option in both the sections (**NNMi Server: Information Required by IPT iSPI** and **IPT iSPI Server: Information Required by NNMi**). Selecting this option ensures

that NNMi and the NNM iSPI for IP Telephony always use the secure mode of communication (HTTPS).

Note: After installing the NNM iSPI for IP Telephony, if you want to change your mode of communication, follow the instructions listed in the Updating the Security Mode (HTTP or HTTPS) section.

10. Click **OK**. This initiates the installation process to completion. After the installation is complete, a message is displayed informing you that the installation process is complete and that you can manually start the NNM iSPI for IP Telephony processes.
11. Click **OK**. You can do the following:
    - Click the **Summary** tab to check if the installation is successful.
    - Click the **Details** tab to verify if the NNM iSPI for IP Telephony packages are successfully installed.
    - Click the **View log file** link in the window to check the log details and errors, if any.
12. Click **Done**. This completes the installation process.

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

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 the problems that caused an unsuccessful installation.

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

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

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, 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 `ovstart -c iptjboss` 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
   ```

Stop the NNM iSPI for IP Telephony processes with the following command:

```
ovstop -c iptjboss
```

However, if you are using the Oracle RAC option, you must perform the following before starting the `iptjboss` process:

- Modify the `$NNMDataDir/nmsas/ipt/server.properties` file by adding the following:
  - `com.hp.ov.nms.oracle.otherHost=<Hostname/IP Address of the secondary Oracle RAC server>`
  - `com.hp.ov.nms.oracle.serviceName=${com.hp.ov.nms.oracle.sid}`
  - `com.hp.ov.nms.oracle.connection.url=${com.hp.ov.nms.oracle.connection.cluster.url}`

After you modify the file, run the following commands:

- `ovstop –c iptjboss`
- `ovstart –c iptjboss`

Post-Installation Configuration Tasks

After the installation, perform these tasks:

1. Make sure that NNMi has discovered the nodes that host the following IP telephony elements:
   - Cisco Unified Communications Managers
   - Cisco UCMEs
   - Cisco Voice Gateways
   - Cisco SRST routers
   - Cisco Gatekeepers

- Cisco Unity and Unity Connection Devices
- Avaya Media Gateways
- Avaya Communication Managers
- Avaya LSPs
- Nortel Signalling Servers
- Nortel Call Servers
- Nortel Media Gateways
- Microsoft Lync Gateways
- Microsoft Lync Servers
- Acme Session Directors

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

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

     For more information about configuring data access with AXL for Cisco IP telephony, see the *Configuring the NNM iSPI for IP Telephony to Access the AXL Data* topic (*Help for Administrators* > *Cisco IP Telephony* > *Configuring Data Access* > *Configurig the NNM iSPI for IP Telephony to Access the AXL Data*) of the *HP Network Node Manager iSPI for IP Telephony Software Online Help 10.00*.
   - *For Cisco IP Telephony.* Configure data access with SSH:
     - Obtain the SSH credentials to access the Cisco Unified Communications Manager.
     - Configure the NNM iSPI for IP Telephony to access the Cisco Unified Communications Manager data with the help of the SSH protocol.

     For more information about configuring data access with SSH for Cisco IP telephony, see the *Accessing the Cisco Unified Communications Managerwith SSH* topic (*Help for Administrators* > *Cisco IP Telephony* > *Configuring Data Access* > *Accessing the Cisco*

Unified Communications Managerwith SSH) of the *HP Network Node Manager iSPI for IP Telephony Software Online Help 10.00*.

- *For Cisco IP Telephony.* Configure the CDR data access.

  For more information about configuring the CDR data access for Cisco IP telephony, see the *Accessing the CDR Data* topic (*Help for Administrators > Cisco IP Telephony > Configuring Data Access > Accessing the CDR Data*) of the *HP Network Node Manager iSPI for IP Telephony Software Online Help 10.00*.

- *For Avaya IP Telephony.* Configure the CDR data access.

  For more information about configuring the CDR data access for Avaya IP telephony, see the *Accessing the CDR Data* topic (*Help for Administrators > Avaya IP Telephony > Configuring Data Access > Accessing the CDR Data*) of the *HP Network Node Manager iSPI for IP Telephony Software Online Help 10.00*.

- *For Avaya IP Telephony.* Configure the RTP Control Protocol (RTCP) reception.

  For more information about configuring the RTCP reception for Avaya IP telephony, see the *Configuring RTCP Reception* topic (*Help for Administrators > Avaya IP Telephony > Configuring Data Access > Configuring RTCP Reception*) of the *HP Network Node Manager iSPI for IP Telephony Software Online Help 10.00*

- *For Avaya IP Telephony.* HP recommends that you configure the NNM iSPI for IP Telephony to access the Avaya System Access Terminal using the SSH protocol for scalable discovery and the polling of IP addresses of Avaya IP phones.

  For more information, see the *Configuring Data Access* topic for Avaya IP telephony (*Help for Administrators > Avaya IP Telephony > Configuring Data Access*) of the *HP Network Node Manager iSPI for IP Telephony Software Online Help 10.00*.

- *For Microsoft IP Telephony:*

  - Enable the periodic topology discovery.
  - Specify the user exclusion filter.

- *For Acme IP Telephony.* Configure data access with SSH:

  - Obtain the SSH credentials to access the Acme Session Director (SD).
  - Configure the NNM iSPI for IP Telephony to access the Acme SD data with the help of the SSH protocol.

  For more information about configuring data access with SSH for Acme IP telephony, see the *Accessing the Acme Session Director with SSH* topic (*Help for Administrators > Acme IP Telephony > Configuring Data Access > Accessing the Acme Session Director with SSH*) of the *HP Network Node Manager iSPI for IP Telephony Software Online Help 10.00*.

- *For Acme IP Telephony.* Configure the CDR data access.

  For more information about configuring the CDR data access for Acme IP telephony, see the *Accessing the CDR Data* topic (*Help for Administrators* > *Acme IP Telephony* > *Configuring Data Access* > *Accessing the CDR Data*) of the *HP Network Node Manager iSPI for IP Telephony Software Online Help 10.00*.

- *For Acme IP Telephony.* Configure the HDR data access.

  For more information about configuring the HDR data access for Acme IP telephony, see the *Accessing the HDR Data for Acme Session Director* topic (*Help for Administrators* > *Acme IP Telephony* > *Configuring Data Access* > *ccessing the HDR Data for Acme Session Director*) of the *HP Network Node Manager iSPI for IP Telephony Software Online Help 10.00*.

3. Seed the nodes that host the following IP Telephony entities, using the Discovery Configuration form in the NNMi Configuration workspace, if you have not seeded the nodes already:

   - Avaya Communications Manager servers: Each physical server in the duplex redundant pairs of the Primary Servers, and each stand alone Primary Server that is not deployed in the duplex redundant pairs.
   - Avaya H.248 Media Gateways: the G250s, G350s, G450s, and the G700s
   - Avaya LSPs
   - Cisco Unified Communications Manager servers in all the clusters in your environment
   - Cisco Unified Communications Manager Express
   - Cisco Unity and Cisco Unity Connection.
   - Cisco SRST routers
   - Cisco Gatekeepers
   - Cisco Voice Gateways
   - Microsoft Lync Gateways
   - Microsoft Lync Servers
   - Nortel Call Servers, Signaling Servers, and Media Gateways
   - Acme Session Directors

If these nodes are already seeded, 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 are managing a small environment, select these nodes from the NNMi node inventory and do a configuration poll for them.

For more information about seeding nodes and performing configuration polls for the nodes, see the *HP Network Node Manager i Software Online Help 10.00*.

4. Seed the L2/L3 infrastructure devices, such as switches and routers, in your environment.
5. Seed the 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/Update Frontend Communication Configuration** page, of the NNM iSPI for IP Telephony Configuration Console.

Note: You can also use the NNM iSPI for IP Telephony Quick Start Wizard to configure the NNM iSPI for IP Telephonyto monitor and manage the Cisco, Avaya, and Acme IP Telephony infrastructure in your network environment.

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:

- **Acme IP Telephony**

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

- Session Director

- **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

- **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

- **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
  - Lync End Users
  - End User Groups
  - Sites
  - SIP Trunk Configurations
  - Dial Plans
  - Voice Routes
  - Voice Policies

- **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

Integrating MS IPT Proxy with NNM iSPI for IP Telephony

After the installation of NNM iSPI for IP Telephony and the MS IPT Proxy, you must integrate them so that they can communicate with each other. This ensures the discovery and monitoring of the Microsoft Lync Server environment by the NNM iSPI for IP Telephony.

To integrate the MS IPT Proxy with the NNM iSPI for IP Telephony, follow these steps:

1. Log on to the NNMi console as an administrator.
2. From the **Workspaces** navigation pane, click **Configuration** > **iSPI for IP Telephony Configuration** > **Microsoft Configuration**. The NNM iSPI for IP Telephony Microsoft Configuration Console opens.
3. Click **Proxy Communication Configuration**. The NNM iSPI for IP Telephony Microsoft Proxy Communication Configuration form opens. The **Proxy Communication Configuration** tab page displays the list of the proxies that are integrated with the NNM iSPI for IP Telephony.
4. On the **Proxy Communication Configuration** tab page, click (the **New** icon). The **Add/Update Proxy Communication Configuration** page opens.
5. On the page, specify the required details in the fields provided. The following table describes the fields on the page:

Field	Description
Proxy Name	Indicates the name of the MS IPT Proxy. You can give any meaningful name to the proxy; however, you cannot edit this field after the configuration is saved.
Proxy IP Address	Indicates the IP address of the Windows server on which MS IPT Proxy is installed.
Proxy Port	Indicates the port number on which MS IPT Proxy is installed.

Note: You can get the IP address and the port number from the `msipt.proxy.properties` file that is present in the server where you installed MS IPT Proxy. Access this file from the following location in that server:

%NnmDataDir%`\shared\ipt\conf`

6. Click (the **Save** icon) to save the configuration to integrate the proxy with NNM iSPI for IP Telephony.

Note: If you want to integrate more proxies with the NNM iSPI for IP Telephony, repeat the steps from Step 4 through Step 6.

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**.

Note: 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 the 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\RegisteredDevicesCount`

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

- preRemove_ipt.log
- postRemove_ipt.log

Remove the Extension Packs

After uninstalling the NNM iSPI for IP Telephony, you must manually remove the NNM iSPI for IP Telephony extension packs from the NPS system.

To remove the extension packs from the NPS system, follow these steps:

1. Log on to the NPS system as `administrator`.
2. Go to the following directory:

   <NPS_Install_Dir>`\NNMPerformanceSPI\bin`
3. Run the following commands:
   - `uninstallExtensionPack -p Acme_IPT_SD_Call_Reports`
   - `uninstallExtensionPack -p Acme_IPT_SD_SIP_Statistics`
   - `uninstallExtensionPack -p Acme_IPT_SD_Statistics`
   - `uninstallExtensionPack -p Acme_IPT_SD_System_Management`
   - `uninstallExtensionPack -p Avaya_IPT_Calls_Terms_Types`
   - `uninstallExtensionPack -p Avaya_IPT_CDR_Collection`
   - `uninstallExtensionPack -p Avaya_IPT_CMProcOccupancy_Sum`
   - `uninstallExtensionPack -p Avaya_IPT_MGW_Calls`
   - `uninstallExtensionPack -p Avaya_IPT_NWReg_DSP_CODEC_Sum`
   - `uninstallExtensionPack -p Avaya_IPT_PN_Load_Stats`
   - `uninstallExtensionPack -p Avaya_IPT_TG_Calls`
   - `uninstallExtensionPack -p Avaya_IPT_TG_RP_Usage`
   - `uninstallExtensionPack -p Avaya_IPT_Trunk_Activity`
   - `uninstallExtensionPack -p Avaya_RTP_Session_Metrics`
   - `uninstallExtensionPack -p Cisco_IPT_Calls_By_Details`
   - `uninstallExtensionPack -p Cisco_IPT_Calls_By_GWs`
   - `uninstallExtensionPack -p Cisco_IPT_Calls_By_IP_Trunks`

- `uninstallExtensionPack -p Cisco_IPT_Calls_Terminations_Types`
- `uninstallExtensionPack -p Cisco_IPT_GW_BChannel_Activity`
- `uninstallExtensionPack -p Cisco_IPT_GW_Call_Activity`
- `uninstallExtensionPack -p Cisco_IPT_Media_Resources`
- `uninstallExtensionPack -p Cisco_IPT_RAIDStatus`
- `uninstallExtensionPack -p Cisco_IPT_SIPTrunk_Session`
- `uninstallExtensionPack -p Cisco_IPT_TFTP`
- `uninstallExtensionPack -p Cisco_IPT_UCM_Call_Activity`
- `uninstallExtensionPack -p Cisco_IPT_UCM_CTIManagerConnections`
- `uninstallExtensionPack -p Cisco_IPT_UCM_System_Health`
- `uninstallExtensionPack -p Cisco_IPT_UCOS_Services`
- `uninstallExtensionPack -p Cisco_IPT_VM_Systems`
- `uninstallExtensionPack -p Call_Reports`
- `uninstallExtensionPack -p Gateway_BChannel_Activity`
- `uninstallExtensionPack -p Gateway_Statistics`
- `uninstallExtensionPack -p Microsoft_Exchange`
- `uninstallExtensionPack -p Microsoft_Lync`

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

To reinstall the NNM iSPI for IP Telephony with different ports on the same system, follow these steps:

1. Restart the `ovjboss` process by running 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 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 removeApplication ipt`
- `ovstop -c ovjboss`
- `ovstart -c ovjboss`

2. Install and configure the NNM iSPI for IP Telephony to work with different ports.
3. Check if you are able to open the NNM iSPI for IP Telephony Configuration Console. If you are not, follow this step:
   - Restart the `ovjboss` and `iptjboss` processes by running the following commands:
     - `ovstop -c ovjboss`
     - `ovstart -c iptjboss`

Updating the Security Mode (HTTP to HTTPS/HTTPS to HTTP)

After installing NNMi and the NNM iSPI for IP Telephony, you can modify the security mode from HTTPS to HTTP or vice-versa, without installing the NNMi and the NNM iSPI for IP Telephony again. To do so, 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`(which indicates an HTTPS mode of communication), or to `false` (which indicates an HTTP mode of communication), 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.`

   Note: Always select the same mode of transmission for NNMi and the 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 to Use SSL)

After installing the NNM iSPI for IP Telephony, if the NPS is configured to use SSL, you must make sure that there is a secure communication (using the HTTPS protocol) between the NPS and the NNM iSPI for IP Telephony server. To achieve this you must export the third-party Cognos certificate and add it to the list of trusted certificates.

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>* indicates the FQDN of the NPS system, and *<nps_https_port>* indicates the HTTPS port that NPS uses for secure communication—the default port is 9305.

2. View the certificate and export it as a DER-encoded binary file.

3. Name the file as "`npscert.cer`".

   Note: You can ignore any warning message that appears while exporting and naming the file.

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

Adding the Cognos Certificate to the List of Trusted Certificates

To add the exported Cognos certificate to the list of trusted certificates, follow these steps:

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 to the `nnm.truststore` location:

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

Note: You can ignore any warning message that appears while running this command.

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

   %NnmInstallDir%`\nonOV\jdk\hpsw\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 the Modified NNMi Ports

After installing the NNM iSPI for IP Telephony, you can modify the following configuration parameters:

- NNMi HTTP port
- NNMi HTTPS port
- NNMi JNDI port

You can configure the NNM iSPI for IP Telephony to use the modified NNMi ports. To configure, follow these steps:

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. Based on the port that you modified, do one of the following:
   - *If you have modified the NNMi HTTP port.* Replace the value of the `com.hp.ov.nms.spi.ipt.Nnm.port` property with the value of the `nmsas.server.port.web.http` property (obtained in Step 2).
   - *If you have modified the NNMi HTTPS port.* Replace the value of the `com.hp.ov.nms.spi.ipt.Nnm.secureport` property with the value of the `nmsas.server.port.web.https` property (obtained in Step 2).

5. 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 the Modified NNMi Web Services Client User Name and 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, follow these steps:

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, follow these steps:

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

Modifying the NNM iSPI for IP Telephony Ports

The NNM iSPI for IP Telephony uses a set of ports—configured at the time of installation by the installer—for its operation. The installer offers you the option to choose non-default values for the HTTP and HTTPS ports. The list of these ports are available in the `server.properties` file—under the*%nnmdatadir%*`\nmsas\ipt`directory. However, after the installation, you can configure the NNM iSPI for IP Telephony to use HTTP and HTTPS ports that are different from the configured ones at the time of the installation.

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. Open the `server.properties` file with a text editor from the *%nnmdatadir%*`\nmsas\ipt` directory.
3. Based on the port that you want to modify, do one of the following:
   - *To modify an HTTPS port.* Replace the value of the `nmsas.server.port.web.https` property with the new HTTPS port.
   - *To modify an HTTP port.* Replace the value of the `nmsas.server.port.web.http` property with the new HTTP port.
4. Save the file.
5. Restart theNNM iSPI for IP Telephony with the following commands:
   a. `ovstop -c ovjboss`
   b. `ovstart -c iptjboss`

Modifying the Embedded Database Port

To configure the NNMi embedded database to use a port different from the one configured during 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 theNNM iSPI for IP Telephony with the following commands:

   a. `ovstop -c ovjboss`

   b. `ovstart -c iptjboss`

Chapter 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, depending on the type of network that you want to monitor, click one of the following, and then click the individual views to see the details of the discovered network and devices:
   - **Acme IP Telephony**
   - **Avaya IP Telephony**
   - **Cisco IP Telephony**
   - **Nortel IP Telephony**
   - **Microsoft IP Telephony**

Accessing the Online Help

To view the details displayed by individual views and forms that are introduced by the NNM iSPI for IP Telephony, see the *NNM iSPI for IP Telephony Online Help*.

To launch the *NNM iSPI for IP Telephony Online Help*, on the NNMi user interface, 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.

Chapter 5: 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 modify the `run.sh` file present in the *%nnmdatadir%*`\shared\ipt\conf` directory.

To modify the file, follow these steps

1. Stop the NNM iSPI for IP Telephony processes by using the following command:

   ```
   ovstop -c iptjboss
   ```

2. From the*%nnmdatadir%*`\shared\ipt\conf` location, open the `run.sh` file.
3. Change the `Djava.net.preferIPv4Stack=true` to `Djava.net.preferIPv4Stack=false.`
4. Restart the `iptboss` processes by using the following command:

   ```
   ovstart -c iptboss
   ```

Starting the NNM iSPI for IP Telephony

1. ***Problem:*** 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.

   To resolve this problem, follow these steps:

a. Make sure that you have installed all the necessary patches for NNMi. For more information, see the *HP Network Node Manager i Software 10.00 Interactive Installation Guide for Windows* .

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 `server.properties` file present under the *%nnmdatadir%*`\nmsas\ipt` directory.

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

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.

2. ***Problem:*** After starting the `iptjboss` process, the process displays its status as `RUNNING` even if the process fails to start.

   Workaround: This problem might occur when the `iptjboss` fails to start due to installation issues, port conflicts, or authentication issues.

   To resolve this problem, follow these steps:

   a. Check if 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 `nmsiptstart.ovpl`, `nmsiptstop.ovpl`, or `nmsiptstatus.ovpl` scripts, do the following for issues related to authentication or port numbers:

      - Update the proper user name and password using the `encryptiptpassword.ovpl` script
      - Update the port numbers in the `server.properties` file and the `nnm.extended.properties` file present in the *%nnmdatadir%*`\nmsas\ipt` directory.

3. ***Problem:*** 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. If you do not find the `Shutdown Complete` message, 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.

   If the `iptjboss` process is still running, follow these steps:

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

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

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

4. ***Problem:*** Multiple instances of the `iptjboss` process resulting in the 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. However, when the `ovstart` command is executed, it 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. If you do not find the `Shutdown Complete` message, 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.

   If the `iptjboss` process is still running, follow these steps, and then start the process:

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

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

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

5. ***Problem:*** The installation of the NNM iSPI for IP Telephony stops abruptly.

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

6. ***Problem:*** The NNM iSPI for IP Telephony forms (including the Configuration forms) 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, the NNM iSPI for IP Telephony forms open with the old port setting, and as a result, the error message regarding the connection appears in the browser.

   To resolve this, follow these steps:

   a. Log on to the management server as `administrator`.

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

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

Removing the NNM iSPI for IP Telephony

1. ***Problem:*** The uninstallation process does not end after starting.

   Solution: To resolve this problem, follow these steps:

   a. Make sure that all the NNMi processes are running.

   b. Stop the `iptjboss` process with the **`ovstop -c iptjboss`** command, and then try to remove the iSPI with the uninstallation wizard.

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

   Solution: To remobve the status of `iptjboss`, run the following commands in the given sequence:

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

We appreciate your feedback!

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Installation Guide (Network Node Manager iSPI for IP Telephony Software 10.00)

Just add your feedback to the email and click send.

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