

# HP Network Node Manager iSPI for IP Telephony Software

for the Windows<sup>®</sup> operating system

Software Version: 9.10

---

## Installation Guide

Document Release Date: March 2011  
Software Release Date: March 2011



## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notices

© Copyright 2008-2011 Hewlett-Packard Development Company, L.P.

### 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.

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

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:

**[www.hp.com/go/hpsoftwaresupport](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 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](http://h20230.www2.hp.com/new_access_levels.jsp)**

# Contents

<b>1</b>	<b>Introduction</b> .....	<b>7</b>
	IP Telephony Workspaces .....	7
	Related Documentation .....	8
<b>2</b>	<b>Before You Begin</b> .....	<b>9</b>
	Installation Plan on the NNMi Management Server .....	9
	Check System Requirements .....	10
	Preinstallation Tasks .....	10
<b>3</b>	<b>Installing the NNM iSPI for IP Telephony</b> .....	<b>13</b>
	Installing on the Management Server .....	13
	Creating the Proxy Service .....	16
	FTP Server Configuration .....	17
	Starting the NNM iSPI for IP Telephony .....	17
	Post-Installation Configuration Tasks .....	18
	Verifying the Installation .....	19
	Removing the NNM iSPI for IP Telephony .....	20
	Remove the Extension Packs .....	21
	Reinstall the NNM iSPI for IP Telephony with Different Ports .....	21
	License Information .....	23
	Checking the License Type .....	24
	Installing the NNM iSPI for IP Telephony Migration Licenses: .....	24
	Installing the iSPI Points Licenses .....	25
	Obtaining the NNM iSPI for IP Telephony Migration Licenses or iSPI Points Licenses .....	25
	Updating the Security Mode (HTTP to HTTPS) .....	25
	Configuring NNM iSPI for IP Telephony to Use Modified NNMi Ports .....	26
	Configuring NNM iSPI for IP Telephony to Use Modified NNMi Web Services Client User Name and or Password .....	26
	Modifying NNM iSPI for IP Telephony Ports .....	27
	Accessing Installation Log Files .....	28
	Troubleshooting Tips .....	28
<b>4</b>	<b>Installing in a High-Availability Cluster or an Application Fail-over Environment</b> .....	<b>31</b>
	Prerequisites .....	31
	Installing the iSPI in an HA Environment .....	31
	Configuring and Unconfiguring the iSPI in the HA Environment .....	31
	Removing the iSPI in an HA Environment .....	32

5 Getting Started with the iSPI for IP Telephony .....	33
Accessing the iSPI for IP Telephony .....	33
Accessing the Online Help .....	33

# 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, Cisco, 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 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 Avaya, Cisco, Microsoft and Nortel IP Telephony networks.

## IP Telephony Workspaces

The NNM iSPI for IP Telephony introduces four new workspaces in the Workspaces pane in the NNMi console: **Avaya IP Telephony**, **Cisco 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 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 9.10 Installation Guide for Windows or HP Network Node Manager i Software 9.10 Installation Guide for UNIX*
- *HP Network Node Manager i Software 9.10 Deployment Reference Guide*
- *HP Network Node Manager i Software 9.10 Release Notes*
- *HP Network Node Manager i Software 9.10 Support Matrix*
- *HP Network Node Manager iSPI Performance for Metrics Software/Network Performance Server Installation Guide*
- *HP Network Node Manager iSPI Performance for Metrics Software/Network Performance Server Support Matrix*
- *HP Network Node Manager iSPI Performance for Metrics Software/Network Performance Server Release Notes*

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

### Installation Plan on the NNMi Management Server

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

#### Database Details

NNMi installer installs a default database that is embedded with the product. However, to achieve higher scalability, you can choose an external Oracle database instead of the embedded database to store NNMi data. See the *HP Network Node Manager i Software 9.10 Installation Guide* for more information on configuring NNMi with Oracle. You must note down the following details of the NNMi database:

- **Type:** The default embedded database or Oracle.
- **Port:** *Only for Oracle.* The port used by the Oracle database.
- **Hostname:** *Only for Oracle.* This is applicable when you use an Oracle database residing on a remote server. Note down the fully-qualified domain name of the database server.

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

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

### NNMi Installation

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

### iSPI Performance for Metrics

You must make sure that the iSPI Performance for Metrics is running if this application is a part of your deployment environment. This component is required to view reports.

### Uninstalling Existing Extension Packs

If there are existing instances of the extension packs on your system. Make sure that you uninstall the extension packs by following the steps listed in the section: [Remove the Extension Packs](#) on page 21.

## 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 a complete information on hardware and software requirements and dependencies.

**Table 1 Preinstallation Checklist for Hardware and Software Requirements**

Requirement	Reference Document	Complete? (Yes/No)
Disk space	<i>HP Network Node Manager iSPI for IP Telephony Software Support Matrix</i>	
Operating system	<i>HP Network Node Manager iSPI for IP Telephony Software Support Matrix</i>	
Database	<i>HP Network Node Manager iSPI for IP Telephony Software Support Matrix</i>	
Browser	<i>HP Network Node Manager iSPI for IP Telephony Software Support Matrix</i>	

# Preinstallation Tasks

Before you begin installation, perform these tasks:

**Task 1:** *Only for Monitoring the Microsoft Lync Server Environment.* Install Microsoft .NET Framework 3.5 (or Higher) on the NNMi Management Server

If you want to monitor the Microsoft Lync Server environment with the iSPI for IP Telephony, Microsoft .NET Framework 3.5 (or higher) must be installed on the management server before installing the iSPI for IP Telephony.

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 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:

1 Configure NNMi to use a non-default HTTP port.

To configure 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 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
```

2 Obtain the Microsoft .NET Framework 3.5 (or higher) installer.

3 Install Microsoft .NET Framework 3.5 (or higher) on the system.

**Task 2:** *Only for Monitoring the Microsoft Lync Server Environment.* Install Microsoft PowerShell 2.0 on the NNMi Management Server

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

**Task 3:** *Only for Monitoring the Microsoft Lync Server Environment.* Specify the Community Strings of Microsoft Lync Servers and Gateways

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 4:** 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 iSPI for IP Telephony.

**Task 5:** *Only for Oracle.* Create a New Oracle Instance

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

**Task 6:** Configuration Tasks on NNMi

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 discovery of non-SNMP nodes that host IP Phones in your network. You can do this by using the Discovery Configuration form in the NNMi Configuration workspace and adding the auto-discovery rules. You must specify the auto-discovery rules in a manner that covers the range of IP addresses for all the possible IP addresses of the IP Phones in your environment. For more information about specifying automatic discovery rules, see the *NNMi Online Help for Administrators*.
- Specify the SNMP v1/v2 community strings: Obtain the SNMP v1/v2 read community strings for all the IP Telephony nodes (for example, the Avaya Communication Manager Server nodes, the Avaya LSP nodes, the Avaya Media Gateway nodes, the Cisco Unified Communications Manager nodes, the Cisco Voice Gateway nodes, the Cisco SRST nodes, the Cisco Call Manager Express nodes and so on). Use the Communication Configuration form in the NNMi Configuration workspace to add these community strings in list of default read community strings to be used by NNMi and NNM iSPI for IP Telephony for SNMP v1/v2-based communication. For more information about specifying SNMP v1/v2 community strings, see the *NNMi Online Help for Administrators*.
- Specify the communication configuration for Avaya Communication Manager servers: It is recommended that NNMi and the NNM iSPI for IP Telephony are configured to use either SNMP v1 or SNMP v3 for communication with Avaya Communications Manager server nodes in your deployment environment. It is also recommended that SNMP queries do not use SNMP `GetBulk` while communicating with these nodes. To enforce this restriction and consistent behavior of SNMP agents on the Avaya Communications Manager server nodes, use the Communication Configuration form in the NNMi Configuration workspace and specify Regions that include this exclusive specification of communication configurations only for the desired set of Avaya Communications Manager Server nodes. Note that you will have to complete this configuration task for all the Avaya Communications Manager server nodes, including each physical server in duplex redundant pairs of Primary Servers, each stand-alone Primary Server that is not deployed in duplex redundant pairs, and each Local Survivable Processor (LSP) server node in your environment. For better consistency in request response sessions, it is also recommended that you set up the regions in such a way that NNMi and 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*.

# 3 Installing the NNM iSPI for IP Telephony

You can install the NNM iSPI for IP Telephony on the NNMi management servers. You can use the installation wizard for installation. 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 with the Administrator privileges.
- 2 Insert the iSPI installation DVD into the DVD drive. The installation wizard opens.
- 3 If the installation wizard does not open automatically, double-click the `setup.exe` file in the root directory of the media. The installation wizard opens.
- 4 In the Introduction screen of the installation wizard, click **Next**. The License Agreement screen appears.
- 5 In the License Agreement screen, select the **I Accept...** option, and then click **Next**. The Product Customization screen appears.
- 6 Select one of the following options from the **Choose the database type** section on the Server Configuration page and click **Next**:
  - **HP Software Embedded Database**
  - **Oracle**
- 7 If you selected **Oracle** in the previous step, you must specify the following details in the screens that follow. You can go to *step 8* if you selected the **HP Software Embedded Database** option:
  - Database Initialization Preferences: Select **Primary Server Installation** or **Secondary Server Installation** based on what you have configured for NNMi installed on this system.
  - Database Server Information to Connect to: Specify the following details to connect to the Oracle database server you have configured for NNMi:
    - **Host**: The fully-qualified domain name of the Oracle server.
    - **Port**: The port number used by the Oracle database server.

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

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

- Database User Account Information: specifies the user account information required to access the Oracle database. you must specify the following details:
  - **Username:** User name to access the Oracle database instance.
  - **Password:** Password for the specified user name.
- 8 Click **Next**. The Install Checks screen appears. The wizard checks for the available disk space.
- 9 After the check is complete, click **Next**. The Pre-Install Summary screen appears.
- 10 Review the options, and then click **Install**. The installation process begins.

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

- 11 Specify the following details:

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

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

- ▶ • The NNM iSPI for IP Telephony installer detects the values listed above based on the values currently used by NNMi.
- ▶ • If the values listed above are modified by the NNMi administrator after the installation of the NNM iSPI for IP Telephony, you must reconfigure the NNM iSPI for IP Telephony to use these updated values. See section [Configuring NNM iSPI for IP Telephony to Use Modified NNMi Ports](#) on page 26 for detailed instructions.
  - Web Service Client Username—specify the NNMi Web Service Client user name. Use the Web Client user you created.
  - Web Service Client Password—password for the above user.
  - Retype Password—retype the password to confirm the password.
- ▶ • If you want to use a different user name or if you change the password after installation of the NNM iSPI for IP Telephony, you must reconfigure the NNM iSPI for IP Telephony to use these updated values. See section [Configuring NNM iSPI for IP Telephony to Use Modified NNMi Web Services Client User Name and or Password](#) on page 26 for detailed instructions.

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

➤ • If you want to change your mode of communication after installation of the NNM iSPI for IP Telephony see section [Updating the Security Mode \(HTTP to HTTPS\)](#) on page 25 for detailed instructions.

- **Information required by NNMi to Communicate with NNM iSPI for IP Telephony**

- IPT FQDN—the fully-qualified domain name of the NNM iSPI for IP Telephony.
- IPT HTTP Port—the HTTP port of the NNM iSPI for IP Telephony.
- IPT HTTPS Port—the HTTPS port of the NNM iSPI for IP Telephony.
- IPT JNDI Port—the JNDI port of the NNM iSPI for IP Telephony.

➤ The NNM iSPI for IP Telephony installer displays the default values for the ports listed above. You can specify the values of your choice. If you want to modify these values after installing the NNM iSPI for IP Telephony, see section [Modifying NNM iSPI for IP Telephony Ports](#) on page 27 for detailed instructions.

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

➤ • If you want to change your mode of communication after installation of the NNM iSPI for IP Telephony see section [Updating the Security Mode \(HTTP to HTTPS\)](#) on page 25 for detailed instructions.

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

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

- Run the `nnmofficialfqdn.ovpl` command.
- From the NNMi console, click **Help > About Network Node Manager i Software**.

The Single Sign-on feature is disabled by default. To enable the Single Sign-on feature, see the *Using Single Sign-On with NNMi* topic in the *Network Node Manager i Software Deployment Reference*

12 Click **Submit**.

13 When the installation process is complete, 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 16 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.

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 at the following location: %temp% to identify any problems that might have occurred which caused an unsuccessful installation.



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

- preInstall\_ipt.log
- postInstall\_ipt.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 17 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 %nnminstalldir%\shared\ipt\conf.
  - b Open the msipt.proxy 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**
  - **Confirm 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 %nnminstalldir%\shared\ipt\conf.
- 3 Open the msipt.proxy 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 present at the directory `%nmninstalldir%\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, do as follows:

- 1 Open the list of services running on the system. You can execute `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.

## FTP Server Configuration

You must configure an FTP server on the management server. The iSPI for IP Telephony collects the CDR files from the CDR Repository Server using one of the following methods:

- Using the `CDRonDemand Web Service`
- Using the `Billing Server-based collection mode`

In case of the `CDRonDemand Web Service` based collection method, the iSPI for IP Telephony pulls the CDR files using the Web Service calls on the `CDRonDemand Web Service`.

In case of the `Billing Server-based collection mode`, the user must configure the NNMi hostname as the billing server along with the FTP information on the Cisco Unified Communications Manager cluster CDR Repository Server administration Web page.

Both the collection methods send the CDR files from the Cisco Unified Communications Manager clusters to the NNMi iSPI for IP Telephony using this FTP server. You must create at least one user on this FTP server and specify the credentials for the user in the NNMi iSPI for IP Telephony Configuration form when specifying the data access configuration.

If the NNMi iSPI for IP Telephony is installed on a Microsoft Windows operating system, you must make sure that the home directory for the user specified in FTP user name is configured as `%nnmdatadir%\log\ipt\tmp` and the user has `write` access to the home directory.

## 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 you installed the proxy service ([Creating the Proxy Service](#) on page 16), starting the `iptjboss` process also starts the `msproxy` service. Stopping the `msproxy` service also stops the `iptjboss` process.

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

**Task 1:** Seed the nodes that host the following IP Telephony Entities using the Discovery Configuration form in NNMi Configuration workspace if you have not seeded the nodes already:

- L2/L3 infrastructure devices such as switches and routers in your environment
- Avaya Communications Manager servers - each physical server in duplex redundant pairs of Primary Servers, each stand alone Primary Server that is not deployed in duplex redundant pairs, and each Local Survivable Processor (LSP) servers in your environment
- Avaya H248 Media Gateways - the G250s, G350s, G450s, and the G700s
- Cisco Unified Communications Manager (Call Manager) Servers in all the clusters in your environment
- Cisco Voice Gateways
- Cisco Gatekeepers
- Cisco SRSTs and Cisco Call Manager Express services
- Cisco Unity servers
- Nortel Call Servers, Signaling Servers, and Media Gateways.

If the above mentioned nodes are already seeded, then you can wait for the next discovery of these nodes by NNMi to trigger a corresponding discovery of the 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 *NNMi Online Help* for more information on seeding nodes and performing configuration polls for nodes.

### 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*.

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

*For the Cisco, Nortel, or Avaya infrastructure*

- IP Phone exclusion filter configuration
- Data access configuration

See the **NNM iSPI for IP Telephony Online Help > Help for Administrators** for more information.

*For the Microsoft infrastructure*

- Enable the periodic topology discovery
- Specify User exclusion filter

See the **NNM iSPI for IP Telephony Online Help > Help for Administrators** for more information.

## 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:

- Call Controllers
- IP Phones
- IC Trunks
- Gatekeepers
- Voice Gateways
- Unity Devices
- Route Group P.01 GoS Summary
- Route List P.01 GoS Summary

- 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 with the Administrator privileges.
- 2 Stop the NNM iSPI for IP Telephony processes with the `ovstop -c iptjboss` command.
- 3 Run the following command at the command prompt:



Alternatively, you can use the command `ovstop -c msproxy` to stop the iSPI for IP Telephony processes. This command works only if you have enabled the `msproxy` service on your system. Stopping the `msproxy` service also stops the `iptjboss` process.

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

A wizard opens.

Alternatively, you can launch the wizard by inserting the NNM iSPI for IP Telephony DVD into the DVD drive, and then running the `setup.bat` or `setup` file (as applicable).

- 4 Follow the instructions on the wizard and complete the procedure to remove the 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`

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



Make sure that no iSPI for IP Telephony extension packs (`<extension_Pack_name>.tar.gz.processed` and `<extension_Pack_name>.tar.gz`) are present at the following location: `%nnmdatadir%\shared\perfSpi\datafiles\extension\final`. In case, the extension packs are present at this location, you must delete these extension packs from the location specified. You must make sure that you delete the `<extension_Pack_name>.tar.gz.processed` files first before deleting the `<extension_Pack_name>.tar.gz` files. `<extension_Pack_name>` refers to the name of the extension pack. See step 3 below for the names of 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 administrator privileges.
- 2 Go to the following directory:

```
<NPS_Install_Dir>\NNMPerformanceSPI\bin
```

- 3 Run the following commands:

- `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 Call_Reports`
- `uninstallExtensionPack -p Cisco_IPT_BChannel_Activity`
- `uninstallExtensionPack -p Cisco_IPT_Calls_Terminations_Types`

- `uninstallExtensionPack -p Cisco_IPT_CDR_Collection`
- `uninstallExtensionPack -p Cisco_IPT_GW_Calls`
- `uninstallExtensionPack -p Cisco_IPT_IP_Trunk_Calls`
- `uninstallExtensionPack -p Cisco_IPT_VM_Information`
- `uninstallExtensionPack -p Gateway_Statistics`
- `uninstallExtensionPack -p Microsoft_Exchange`
- `uninstallExtensionPack -p Microsoft_Lync`

## Reinstall the NNM iSPI for IP Telephony with Different Ports

If you want to reinstall the NNM iSPI for IP Telephony with different ports, follow these steps:

- 1 Before reinstalling the iSPI, run the following commands:

- `%nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password> -s <nnmi_host_fqdn>:<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> -s <nnmi_host_fqdn>:<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> -s <nnmi_host_fqdn>:<nnmi_jndi_port> invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplicationService ipt <nnmi_host_fqdn> https <iSPI_https_port>`
- `%nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password> -s <nnmi_host_fqdn>:<nnmi_jndi_port> invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplicationService msipt <nnmi_host_fqdn> https <iSPI_https_port>`
- `%nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password> -s <nnmi_host_fqdn>:<nnmi_jndi_port> invoke com.hp.ov.nms.topo:service=NetworkApplication removeApplication ipt`
- `%nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password> -s <nnmi_host_fqdn>:<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 and iptjboss processes by running the following commands:
  - **ovstop -c ovjboss**
  - **ovstart -c iptjboss**
- 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:
    - **%nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password> -s <nnmi\_host\_fqdn>:<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> -s <nnmi\_host\_fqdn>:<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> -s <nnmi\_host\_fqdn>:<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> -s <nnmi\_host\_fqdn>:<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 previous versions (7.xx) 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 Smart Plug-ins 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 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 (depending on the type of the management server) with a text editor.
- 2 Update the values to true or false from the following:
  - `com.hp.ov.nms.spi.ipt.Nnm.isSecure=false`: To modify the mode of communication used by iSPI for IP Telephony to communicate with NNMi.
  - `com.hp.ov.nms.spi.ipt.spi.isSecure=false`: To modify the mode of communication used by NNMi to communicate with the iSPI for IP Telephony.

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



Always select the same mode of transmission for NNMi and 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`

## Configuring 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, HTTPS port, and JNDI 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: `jboss.http.port`, `jboss.https.port`
- 3 Replace the value for `-Djboss.nm.port` property with the value of the `jboss.http.port` obtained in the previous step in the `nms-ipt.ports.properties` file present in the `%nnmdatadir%\shared\ipt\conf` directory.
- 4 Replace the value for `com.hp.ov.nms.spi.ipt.Nm.port` property with the value of the `jboss.http.port` obtained in the previous step in the `nm.extended.properties` file present in the `%nnmdatadir%\shared\ipt\conf` directory.
- 5 Replace the value for `com.hp.ov.nms.spi.ipt.Nm.secureport` property with the value of the `jboss.https.port` obtained in the previous step in the `nm.extended.properties` file present in the `%nnmdatadir%\shared\ipt\conf` directory.
- 6 Restart the NNM iSPI for IP Telephony with the following commands:
  - a `ovstop -c iptjboss`
  - b `ovstart -c iptjboss`

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



If you want to change the port of the proxy service, see [Changing the Port of the Proxy Service](#) on page 16.

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

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

1 Run the following commands:

- `%nnminstalldir%\support\nnmtwiddle.ovpl -u <username> -p <password> -s <nnmi_host_fqdn>:<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> -s <nnmi_host_fqdn>:<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> -s <nnmi_host_fqdn>:<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> -s <nnmi_host_fqdn>:<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

- 2 Replace the value for `-Djboss.http.port` and `-Djboss.https.port` properties with the new values in the `nms-ipt.ports.properties` file present in the `%nnmdatadir%\shared\ipt\conf` directory.
- 3 Replace the value for `com.hp.ov.nms.spi.ipt.spi.port` property and the `com.hp.ov.nms.spi.ipt.spi.secureport` property with the new values in the `nm.extended.properties` file present in the `%nnmdatadir%\shared\ipt\conf` directory.
- 4 Restart the `ovjboss` and `iptjboss` processes with the following commands:
  - a `ovstop -c ovjboss`
  - b `ovstart -c iptjboss`

## Accessing Installation Log Files

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

## 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 `jbossServer.log` file present in the `ipt` log folder present at the following location: `%nnmdatadir%\log\ipt` for any entry specified as `ROOT CAUSE` in the deployment of Java MBeans. If there are any port conflicts, you can edit the values in the `nms-ipt.ports.properties` file present under the following directory:  
`%nnmdatadir%\shared\ipt\conf`
- c Check the `iptjboss` startup process by running the `nmsiptstart.ovpl` script present under the following directory: `%nnminstallmdir%\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> -s <nnmi_host_fqdn>:<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> -s <nnmi_host_fqdn>:<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> -s <nnmi_host_fqdn>:<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> -s <nnmi_host_fqdn>:<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 Installing in a High-Availability Cluster or an Application Fail-over Environment

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

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

### Prerequisites

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

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

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

### Installing the iSPI in an HA Environment

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

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

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

### Configuring and Unconfiguring the iSPI in the HA Environment

Use the following command to configure NNM iSPI for IP Telephony:

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

Use the following command to unconfigure the iSPI:

```
%nnminstalldir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon IPT
```

## Removing the iSPI in an HA Environment

To remove the iSPI, follow these steps:

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

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



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



# 5 Getting Started with the iSPI for IP Telephony

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

## Accessing the iSPI for IP Telephony

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

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

## Accessing the Online Help

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

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

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



## 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:**

**Document title:**

**Feedback:**

