HP NNM iSPI Network Engineering Toolset

for the Windows operating system

Software Version: 8.1x Patch 4 (8.12)

Planning and Installation Guide

hp ®

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, 2009 Hewlett-Packard Development Company, L.P.

Trademark Notices

DOM4J® is a registered trademark of MetaStuff, Ltd.

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

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

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

UNIX® is a registered trademark of The Open Group.

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

This product includes ASM Bytecode Manipulation Framework software developed by Institute National de Recherche en Informatique et Automatique (INRIA). Copyright © 2000-2005 INRIA, France Telecom. All Rights Reserved.

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.

The following table indicates changes made to this document since the last released edition.

Document Changes

Chapter	Version	Changes
All	8.10	First publication
About NNM iSPI NET Components	8.1x Patch 4 (8.12)	NNM iSPI NET Load Custom Attributes on Nodes Command on page 46

Support

Visit the HP Software Support web site at:

www.hp.com/go/hpsoftwaresupport

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

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

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

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

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

To find more information about access levels, go to:

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

Contents

1 Introducing HP NNM iSPI Network Engineering Toolset

The HP NNM iSPI Network Engineering Toolset extends NNMi's powerful network management capabilities by providing additional troubleshooting and diagnostic tools for network engineers. NNM iSPI NET includes:

- Diagnostics flows that automatically gather diagnostic information when NNMi detects certain network incidents

- SNMP trap analytics that provide both summary and detailed information about SNMP trap storms impacting your network

- Troubleshooting tools that do the following:

  — Determine the switch port where a node is attached based on the node's hostname, IP address or MAC address

  — Report all end nodes attached to a switch

How is NNM iSPI NET Installed?

NNM iSPI NET's SNMP trap analytics and troubleshooting tools are automatically installed with NNMi. However, the diagnostic flows and diagnostics server must be installed from a separate installation media. See Chapter 3, Installing and Removing NNM iSPI NET for details.

Licensing

NNM iSPI NET is enabled with a temporary Instant-On license password, valid for 30 days after you install NNMi. A permanent NNM iSPI NET license must be purchased separately from your permanent NNMi license. See License NNM iSPI NET on page 34 for details.

2 Pre-Installation Checklists

This chapter contains checklists for the tasks that you must complete before installing NNM iSPI NET, including where to find information on supported hardware and software.

The NNM iSPI NET SNMP trap analytics and troubleshooting tools are automatically installed during NNMi installation; they share NNMi's installation requirements, documented in the NNMi installation guides.

The NNM iSPI NET diagnostics are installed separately using the NNM iSPI NET installation media. For specific supported configurations, this installation can be on the same system as NNMi. The following section describes how you can determine the hardware and software prerequisites for the NNM iSPI NET diagnostics server.

Supported Hardware and Software

Before installing NNM iSPI NET, read the information about supported hardware and software described in Table 1.

> For the most up-to-date versions of all documents listed here, go to the following web site:
>
> **http://h20230.www2.hp.com/selfsolve/manuals**

Table 1   Software and hardware pre-installation checklist

Complete (y/n)	Documentation to read
	HP NNM iSPI NET Release Notes • **Filename** = releasenotes_en.html • **Media** = NNM iSPI NET 8.10 installation DVD (root directory)
	HP NNM iSPI NET Software System and Device Support Matrix • **Filename** = supportmatrix_en.html • **Media** = NNM iSPI NET 8.10 installation DVD (root directory)

> HP updates the HP NNM iSPI NET Software System and Device Support Matrix as new information becomes available. Before you begin to deploy NNM iSPI NET, check for the most recent NNMi support matrix at this web site:

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

(You must have an HP Passport ID to access this web site.)

NNMi Management Server Preparation

Diagnostics flows require device credentials in order to execute. To specify credentials for a device, follow these steps:

1 Open the NNMi console.

2 Navigate to the **Configuration** workspace.

3 Select the **Communication Configuration** form.

4 Use the **Default Device Credentials** tab to create default device credentials.

5 If there are credentials that differ from the default settings, use the **Regions** and **Specific Node Settings** tabs to define those credentials.

▶ Device credentials are only needed on devices for which diagnostics flows will be executed. See the Supported Hardware and Software on page 11 for details about supported devices.

Diagnostics Server System Preparation

The NNM iSPI NET diagnostics include an embedded version of HP Operations Orchestration Central with restricted capabilities. The NNM iSPI NET diagnostics flows can be run by this embedded diagnostics server or by an HP Operations Orchestration Central already installed in your environment.

If you plan to use the embedded NNM iSPI NET diagnostics server, you must identify a system in your environment on which to install the diagnostics server.

➤ You can install the embedded NNM iSPI NET diagnostics server on the same system as NNMi, *if* NNMi is installed on a Windows system with sufficient resources. To learn more about hardware prerequisites for the diagnostics server, see Supported Hardware and Software on page 11.

Table 2   Diagnostics server preparation checklist

Complete (y/n)	Diagnostics server preparation
	If you plan to use the embedded NNM iSPI NET diagnostics server, identify unused ports that can be assigned as the HTTP and HTTPS port numbers for the diagnostics server. Typical values include the following: • 80 or 8080 for HTTP (default is 8080) • 443 or 8443 for HTTPS (default is 8443)
	If you plan to use an HP Operations Orchestration Central already installed in your environment, you need the following: • The HTTP and HTTPS port numbers used by HP OO Central • The password for HP OO Central's admin user
	If you plan to use an HP Operations Orchestration Central already installed in your environment, you must create new certificate files so that the installer can install diagnostic flows. See Creating Certificate Files on an Existing HP OO Central Server on page 16.

Table 2   Diagnostics server preparation checklist

Complete (y/n)	Diagnostics server preparation
	The NNM iSPI NET diagnostics server requires MySQL. The NNM iSPI NET server installer installs and configures MySQL, if it is not already installed. Alternatively, during installation, you can specify an existing MySQL server to be used by the diagnostics server. If you plan to install MySQL, make sure all prior MySQL program, configuration, and database files have been removed. These will typically be found under a path similar to `C:\Program Files(x86)\MySQL\MySQL Server 5.0\`
	If you want the diagnostics server to use an existing MySQL server instead of installing MySQL, you need the following: • The hostname or IP address of the existing MySQL server • The MySQL database root user name and password (so that the installer can create the needed database) • A database name for the diagnostics server's MySQL database (this database cannot already exist—it will be created during the installation) • A database user name and password for accessing the diagnostics server's MySQL database If the existing MySQL server is installed on a separate system from the NNM iSPI NET diagnostics server, the MySQL server must allow remote access for the database root user.
	Gather the following information on NNMi: • NNMi system hostname or IP address • NNMi server port • NNMi administrative user name and password

Table 2   Diagnostics server preparation checklist

Complete (y/n)	Diagnostics server preparation
	Verify that the diagnostics server system and NNMi agree on the hostname of the diagnostics server system. The installer uses the hostname of the diagnostics server system when generating an SSL certificate. This certificate is used to secure communication between the diagnostics server and NNMi. The hostname in the SSL certificate must match the hostname that NNMi uses for the diagnostic server system. If you are not sure NNMi can identify this hostname as the diagnostic server hostname, follow these steps: 1 Log on to the NNMi system. 2 Ping the diagnostics server using its hostname: — If the ping succeeds and matches the IP address of the diagnostics server system, you have a match. — If the ping fails or has the wrong IP address, you must find a hostname for the diagnostics server system that is recognized by both NNMi and the diagnostics server.
	Install and enable a supported web browser if one is not already installed. For details, see the documents described in Supported Hardware and Software on page 11.

Creating Certificate Files on an Existing HP OO Central Server

If you plan to use an existing HP OO Central server for NNM iSPI NET diagnostics flows, you must create an SSL certificate file for the NNM iSPI NET server installer. The installer looks for this file in a specific location. You must create the file before installing the NNM iSPI NET diagnostics flows.

In addition, NNMi's SSL communication stack enforces hostname verification. However, HP OO Central does not include hostnames in its SSL certificates by default.

Unless you have already done so, you must create an HP OO Central keystore entry that includes hostname. This entry is required to create a valid certificate file for the installer.

➤ The NNM iSPI NET embedded diagnostics server includes a hostname in its default SSL certificates; the information in this section only applies to existing HP OO Central servers. It does not apply to NNM iSPI NET embedded diagnostics servers.

NNMi communicates with the **RSCentral** HP OO Central service (also known as **PAS**). RSCentral communicates with two other HP OO Central services: **RSJRAS** (also known as **RAS**) and **RSScheduler**. The HP OO Central may also communicate with HP OO Studio and RAS clients. The trust relationships between these applications are managed through Java keystores.

The tasks in this section are as follows:

1 Check to make sure your current HP OO Central keystore entry contains a valid hostname.

2 Replace the current HP OO Central keystore entry if it does not contain a valid hostname.

⚠ If you replace the current keystore entry, you must re-establish the trust relationships between the HP OO Central services and between HP OO Central and its clients.

3 Export the keystore entry to the certificate file used by the NNM iSPI NET server installer.

Task 1: Set Environment Variables

The example commands below use environment variables. Set these environment variables as follows:

1 Log in with administrator privileges to the HP OO Central server and bring up a command prompt.

2 HP OO Central sets the system environment variable %ICONCLUDE_HOME% to HP OO Central's installation directory. Use the following command to verify this variable's setting:

```
echo %ICONCLUDE_HOME%
```

This should display a path similar to C:\Program Files\Hewlett-Packard\Operations Orchestration

3   Use the following commands to set %JBIN_DIR%, %PAS_KEYSTORE%, and %HOSTNAME%:

set JBIN_DIR=%ICONCLUDE_HOME%\jre1.6\bin

set PAS_KEYSTORE=%ICONCLUDE_HOME%\Central\conf\ rc_keystore

set HOSTNAME=<server.mycompany.com>

Use the current system hostname for **<server.mycompany.com>**. This value must match the hostname that NNMi uses for the HP OO Central server.

> If you are not sure that NNMi can identify this hostname as the HP OO Central server's hostname, follow these steps:
>
> 1   Log on to the NNMi system.
> 2   Ping the HP OO Central server using its hostname:
>   — If the ping succeeds and matches the IP address of the HP OO Central server, you have a match.
>   — If the ping fails or has the wrong IP address, you must find a hostname for the HP OO Central server that is recognized by both NNMi and the HP OO Central server.

Task 2:   Check the SSL Certificate

Check HP OO Central's keystore entries for hostname as follows:

1   Log in with administrator privileges to the HP OO Central server and bring up a command prompt.

2   In this window, verify and set environment variables as described in Set Environment Variables on page 17.

3   Enter the following Java *keytool* command:

"%JBIN_DIR%"\keytool -list -v -keystore "%PAS_KEYSTORE%" -storepass bran507025

4   Look at the *Owner* and *Issuer* fields in the keystore entry of type *keyEntry*, for example:

```
Entry type: keyEntry
Owner: CN=server.company.com, O=OO, C=SW
Issuer: CN=server.company.com, O=OO, C=SW
```

— If the *keyEntry* does not include the hostname of the HP OO Central server, you must replace it. See Replace the Keystore Entry on page 19.

— If the *keyEntry* includes the hostname of this HP OO Central server, you can use it to generate the nnmgenpas.cer certificate file for the installer. See Create the Certificate File on page 20.

> The *keyEntry* hostname must match the hostname that NNMi uses for the HP OO Central server.

If you are not sure that NNMi can identify this hostname as the HP OO Central server's hostname, follow these steps:

1 Log on to the NNMi system.
2 Ping the HP OO Central server using its hostname:
   — If the ping succeeds and matches the IP address of the HP OO Central server, you have a match.
   — If the ping fails or has the wrong IP address, you must find a hostname for the HP OO Central server that is recognized by both NNMi and the HP OO Central server.

Task 3: Replace the Keystore Entry

NNMi's SSL communication stack enforces hostname verification. However, HP OO Central does not include hostnames in its SSL certificates by default.

The *HP Operations Orchestration Software Administrator's Guide* describes how to replace the HP OO security certificate. Use the procedure in this guide to replace the *keyEntry* in %PAS_KEYSTORE% if it does not include the HP OO Central server's hostname.

Before proceeding with the certificate replacement steps, note the following:

• When you generate the new key pair for %PAS_KEYSTORE%, you must include a valid hostname in the *dname* parameter, for example:

```
"%JBIN_DIR%"\keytool -genkey -dname "CN=%HOSTNAME%, O=OO,
C=SW" -alias nnmi-pas -keypass bran507025 -keystore
"%PAS_KEYSTORE%" -storepass bran507025 -keyalg "RSA"
-validity 5475
```

• The hostname you specify must match the hostname that NNMi uses for the HP OO Central server. See the command for setting %HOSTNAME% under Set Environment Variables on page 17.

- NNMi does not communicate directly with HP OO's RAS service. This means that you can leave your RAS *keyEntry* unchanged. However, you must complete the steps for importing the new PAS certificate into your RAS keystores.

- Signed certificates are more secure; however, you may not require signed certificates in your environment. HP OO Central and NNMi work with both signed and self-signed certificates. If you do not require signed certificates, skip the steps for obtaining signed HP OO certificates.

- The *HP Operations Orchestration Software Administrator's Guide* includes instructions for re-establishing trust relationships and mutual SSL authentication after keystore changes. Follow these instructions, then verify that HP OO Central and its Studio and RAS clients can still communicate.

After replacing the *keyEntry* in %PAS_KEYSTORE%, you can create the certificate file for the NNM iSPI NET server installer.

Task 4: Create the Certificate File

Once the HP OO Central keystore has a *keyEntry* that include the server's hostname, create the certificate file for the NNM iSPI NET server installer. You must create the certificate file using the location and name given in the example command. The NNM iSPI NET server installer uses this pathname to find the certificate file.

Export the %PAS_KEYSTORE% entry to its certificate file as follows:

1 Log in with administrator privileges to the HP OO Central server and bring up a command prompt.

2 In this window, verify and set environment variables as described in Set Environment Variables on page 17.

3 Enter the following Java *keytool* command:

```
"%JBIN_DIR%"\keytool -exportcert -alias nnmi-pas -file
"%ICONCLUDE_HOME%"\Central\conf\nnmgenpas.cer -keypass
bran507025 -keystore "%PAS_KEYSTORE%" -storepass
bran507025
```

▶ Use the appropriate alias instead of **nnmi-pas** if your *keyEntry* has a different alias. See Check the SSL Certificate on page 18.

After you create the `nnmgenpas.cer` file, you can run the NNM iSPI NET server installer. See Chapter 3, Installing and Removing NNM iSPI NET.

For more information on HP OO Central SSL certificates, see the *HP Operations Orchestration Software Administrator's Guide*.

3 Installing and Removing NNM iSPI NET

This chapter guides you through the process of installing and licensing NNM iSPI NET. The final section describes how to remove NNM iSPI NET from your system.

Some NNM iSPI NET components are automatically installed with NNMi. However, the NNM iSPI NET diagnostics include a separately-installed diagnostics server, which is an embedded version of HP Operations Orchestration Central with restricted capabilities. NNM iSPI NET diagnostics flows can be run by this diagnostics server or by an HP Operations Orchestration Central server already installed in your environment.

> If NNMi is installed on a Windows system with sufficient resources, you can install the embedded NNM iSPI NET diagnostics server on the same system (see Chapter 2, Pre-Installation Checklists).

Whether you want to install the NNM iSPI NET diagnostics server or use a pre-existing HP Operations Central, you use the NNM iSPI NET diagnostics server installer. Two installation scenarios are described separately in the following sections:

- If HP Operations Orchestration Central is not installed on the system, the NNM iSPI NET server installer installs the NNM iSPI NET diagnostics in their entirety, including the diagnostics server. The installer also sets up the binding between the diagnostics server and the NNMi server.

- If HP OO Central is already installed, the NNM iSPI NET server installer simply installs the NNM iSPI NET diagnostics flows and sets up the binding between HP OO Central and the NNMi server.

Before you begin, make sure that you have completed the requirements in Chapter 2, Pre-Installation Checklists.

Install NNM iSPI NET

To install NNM iSPI NET, first install NNMi as described in the *NNMi Installation Guide*. This installation automatically provides SNMP trap analytics and the troubleshooting tools. Then you will be ready to install the NNM iSPI NET diagnostics.

Installing NNM iSPI NET Diagnostics on a System Without a Pre-existing HP Operations Orchestration Central

Follow these steps to install the NNM iSPI NET diagnostics server and flows on a system that does not have an HP Operations Orchestration Central already installed:

1   Log in with administrator privileges to the system where you plan to install the NNM iSPI NET diagnostics.

2   Insert the NNM iSPI NET 8.10 installation DVD into the DVD-ROM drive, or download the electronic installation media.

3   In the root directory of the installation media, double-click the setup.exe file.

You see the Installer Welcome window, which lists installation steps on the left side. These steps are described in more detail below.

> If components such as .NET or MySQL are already installed, a check mark indicates these installation steps are complete.
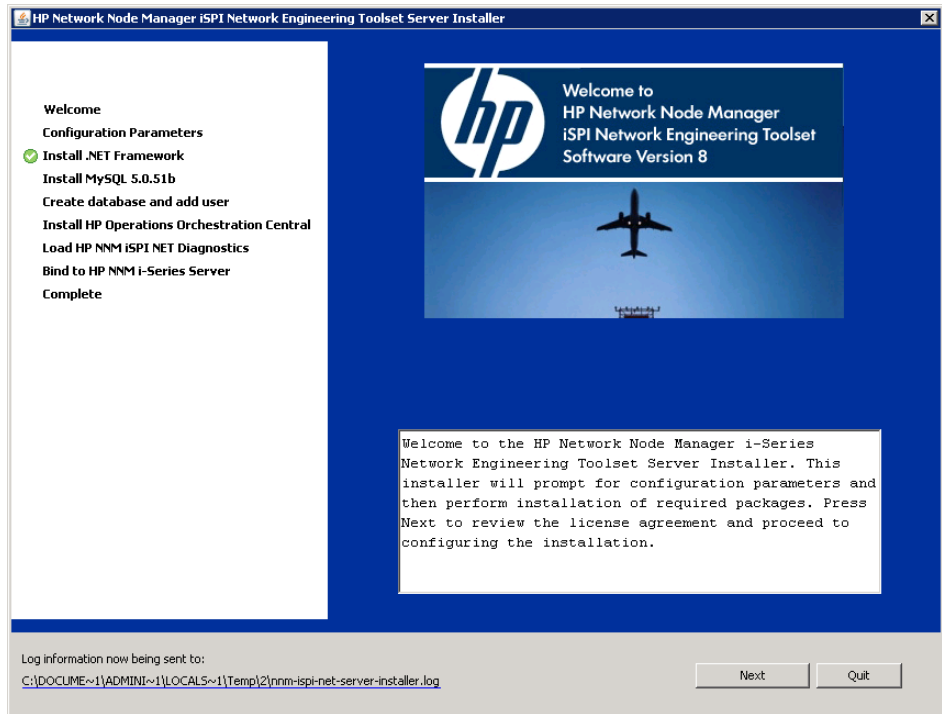
4   Click **Next**; then accept the License Agreement to bring up the
    Configuration Parameters window, as shown below.
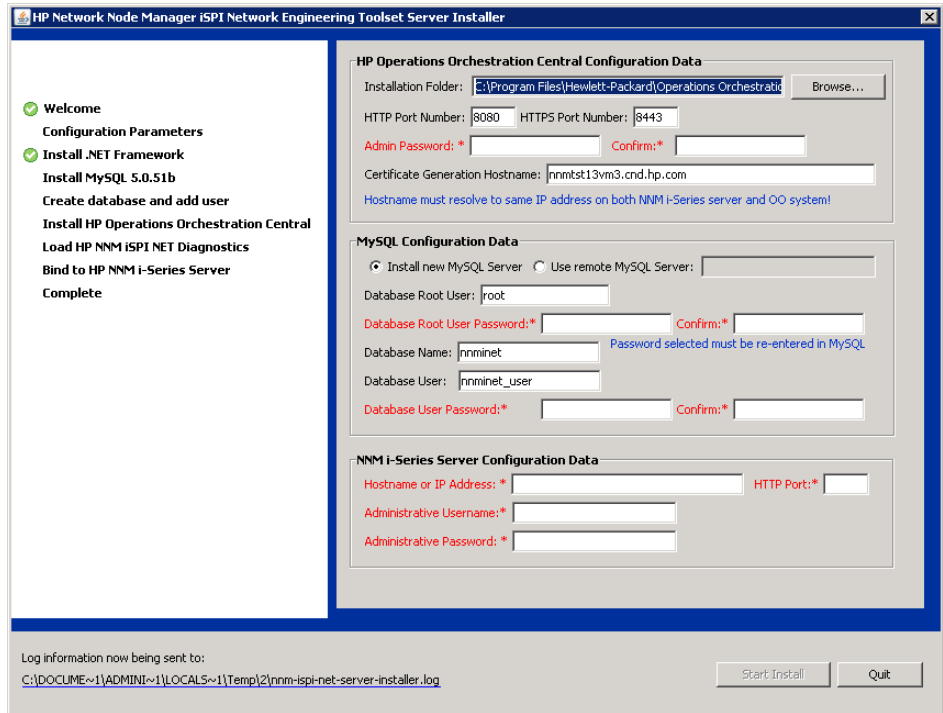
5　Review the fields provided in the Configuration Parameters window and note the following:

- The labels for required fields appear in red text, followed by an asterisk. Once valid data has been entered, the asterisk after the label disappears and the label text turns black.

- If you already have HP Operations Orchestration Central installed on the system, some HP OO Central configuration fields are inactive, such as the Installation Folder and all of the MySQL configuration fields.

- If you are installing a system that does not have HP Operations Orchestration Central, the **HP Operations Orchestration Central Configuration Data** items refer to the diagnostics server. This server is an embedded HP Operations Orchestration Central server. Follow the steps below to provide parameters for installing and configuring this embedded diagnostics server.

6   Configure the diagnostics server as follows:

- Optionally, change the installation directory for the embedded HP Operations Orchestration Central.

- Verify the HTTP and HTTPS port numbers for the HP Operations Orchestration UI and change them if necessary.

  ➤ Communication between the embedded HP OO Central web application and the HP OO Central web client is over secure connections, using the HTTPS protocol. The HTTP port makes it possible for client users to type an HTTP protocol address in the browser and be redirected to the secure connection.

- Enter a password for the diagnostics server *admin* account. At the end of the installation process, you use this password for the user *admin* in the embedded HP OO Central's login window.

- Verify the current system's hostname for SSL certificate generation.

  ➤ If you are installing the NNM iSPI NET diagnostics server on a separate system from NNMi, the hostname in this field must match the hostname that NNMi identifies as the diagnostics server's hostname. If you are not sure that NNMi can identify the diagnostics server's hostname, follow these steps:

    1   Log on to the NNMi system.
    2   Ping the diagnostics server using its hostname:
        — If the ping succeeds and matches the IP address of the diagnostics server system, you have a match.
        — If the ping fails or has the wrong IP address, you must find a hostname for the diagnostics server system that is recognized by both NNMi and the diagnostics server. Use this hostname to replace the Certificate Generation Hostname.

7   Configure MySQL as follows:

- Do one of the following:

    — Select **Install new MySQL Server**.

    — Select **Use remote MySQL Server**, and enter the hostname or IP address of the remote server.

- Optionally, change the database root user name.

- Enter the database root user password.
- Optionally, change the database name.
- Optionally, change the database user name.
- Enter the database user password.

8 Configure the NNMi server as follows:

- Enter the hostname or IP address of your NNMi server.
- Enter the HTTP port used by NNMi.
- Enter the NNMi administrative user name.
- Enter the NNMi administrative user password.

9 Once you fill in the required configuration information, **Start Install** becomes active.

> As with any configuration and set-up procedure, you need to retain the configuration values you entered. Especially, you will need the MySQL root user password again shortly, during the MySQL installation step.

10 Click **Start Install**. You can view the install log file at any time during the installation by clicking on the log file link in the lower-left corner of the Installer window.

11 Unless MySQL is already installed, the MySQL installation begins.

The MySQL installer runs independently from the NNM iSPI NET server installer. Because of this, if you are installing MySQL, you need to do the following:

a Provide MySQL configuration information again (for example, the root database user name).

b Press **Continue** in the NNM iSPI NET server Installer window after MySQL configuration is finished. This ensures that MySQL is active before the NNM iSPI NET server installer accesses it.

The remaining steps of the NNM iSPI NET server installer complete automatically:

- Installing the embedded HP Operations Orchestration Central server
- Loading the NNM iSPI NET diagnostics flows
- Binding to the NNMi server

These steps could take several minutes to complete on a slow system.

12 Once all the installation steps have been completed, a completion message appears in the Installer window and **Finish** becomes active.

> By default, the embedded HP Operations Orchestration Central UI is launched when you click **Finish**. To skip this launch, remove the check mark next to **Launch HP OO**.

13 Click **Finish** to close the Installer window.

If you chose to launch the embedded HP Operations Orchestration Central UI, your browser opens.

You may see an invalid SSL certificate message because the installer includes, by default, a self-signed certificate that serves as a placeholder for a valid customer-obtained certificate. If you choose not to create a signed security certificate for HP OO Central, you can safely ignore this warning.

## Installing the NNM iSPI NET Diagnostic Flows on an Existing HP Operations Orchestration Central Server

1 Log in with administrator privileges to the system running the existing HP OO Central.

2 Insert the NNM iSPI NET 8.10 installation DVD into the DVD-ROM drive, or download the electronic installation media.

3 In the root directory of the installation media, double-click the setup.exe file.

You see the Installer Welcome window, which lists installation steps on the left side. These steps are described in more detail below.

> Because HP Operations Orchestration Central is already installed on this system, check marks indicate installation steps that have already been completed.
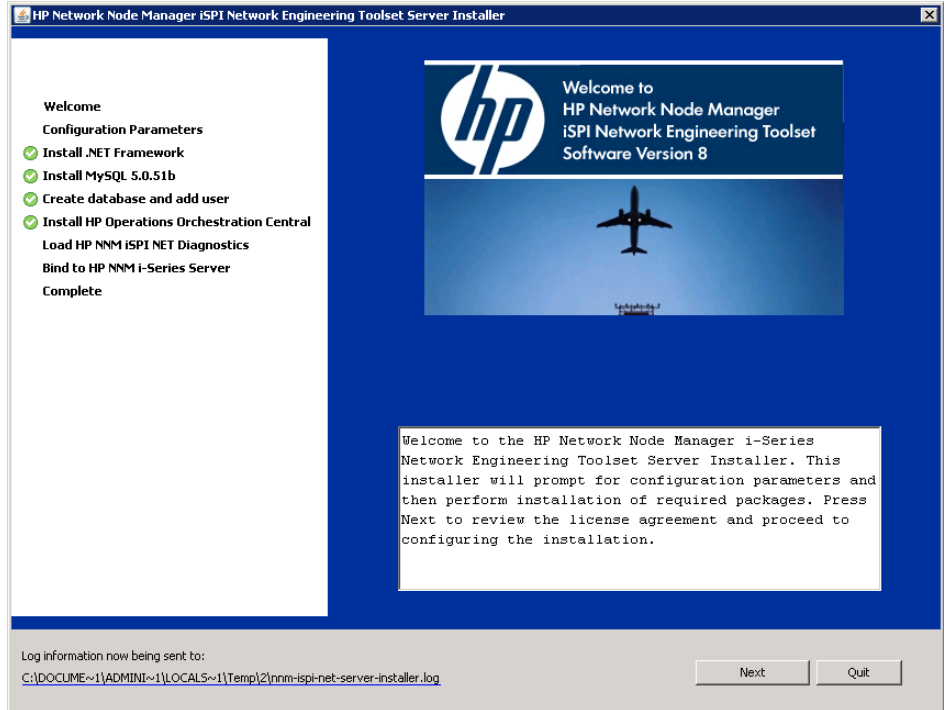
4 Click **Next**; then accept the License Agreement in the pop-up window, to bring up the Configuration Parameters window, as shown below.
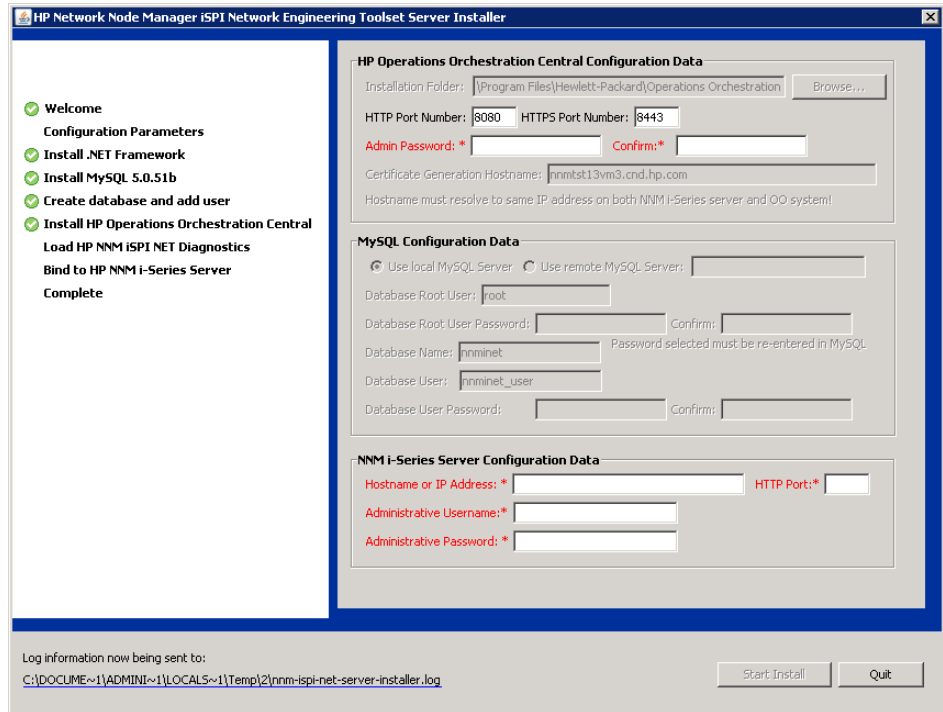
5   Review the fields provided in the Configuration Parameters window and note the following:

• The labels for required fields appear in red text, followed by an asterisk. Once valid data has been entered, the asterisk after the label disappears and the label text turns black.

• Because HP Operations Orchestration Central is already installed on this system, many of the configuration fields are greyed out.

6   Do the following:

- • Verify the HP OO Central HTTP and HTTPS ports and change them if necessary.

    Communication between the embedded HP OO Central web application and the HP OO Central web client is over secure connections, using the HTTPS protocol. The HTTP port makes it possible for client users to type an HTTP protocol address in the browser and be redirected to the secure connection.

- • Enter the password for the HP OO Central admin user.

- • Enter the hostname or IP address, HTTP port, and administrative account information for your NNMi server.

Once you enter the required configuration information, **Start Install** becomes active.

    As with any configuration and set-up procedure, you need to retain the configuration values you entered.

7   Click **Start Install**. The remaining steps of the NNM iSPI NET server installer complete automatically:

- • Loading the NNM iSPI NET diagnostics flows

- • Binding to the NNMi server

You can view the install log file at any time during the installation by clicking on the log file link in the lower left-corner of the Installer window.

8   Once all the installation steps have been completed, a completion message appears in the Installer window and **Finish** becomes active

    By default, the HP Operations Orchestration Central UI is launched when you click **Finish**. To skip this launch, remove the check mark next to **Launch HP OO**.

9   Click **Finish** to close the Installer window.

Creating Users on the Diagnostics Server

To view results from NNM iSPI NET diagnostics flows, NNMi users must launch pages on the server where the diagnostics flows are installed. To do so, these users need user accounts on the diagnostics server.

If you installed the diagnostics flows on a pre-existing HP Operations Orchestration Central server, work with the HP OO Central systems administrator to set up HP OO user accounts.

If you are using the embedded NNM iSPI NET diagnostics server, you should set up user accounts for NNMi users on the diagnostics server. For ease of use, set up the user names and passwords to match pre-existing NNMi user accounts. This best practice makes it easier to update accounts for future releases of NNM iSPI NET.

Setting Up Diagnostics Server User Accounts

To set up user accounts on the diagnostics server:

1 Bring up the diagnostics server login page by entering the following URL into a web browser window:

    http://*<host name>*:*<port>*/PAS/

    Where *<host name>* is the name of the diagnostics server and *<port>* is the port that you specified for the embedded HP Operations Orchestration Central during server installation.

2 Log in as `admin` using the password you specified during installation.

3 From the **Administration** tab, click **Manage Users**.

4 For each user account, do the following:

    • Click **Add New User**.

    • Enter a user account name.

    • Click the checkbox next to **Internal Account**.

    • Enter the account password in the **User Password** and **Verify Password** fields.

    • Click **Create User**.

For more information about HP Operations Orchestration Central users, capabilities, and permissions, see the *Users, groups, and access control* section of the HP Operations Orchestration Central online help.

License NNM iSPI NET

NNM iSPI NET is enabled by a temporary Instant-On license password, valid for 30 days after you install NNMi. A permanent NNM iSPI NET license password must be purchased separately from your permanent NNMi license password. You should obtain and install a permanent license password as soon as possible.

Checking the License Type

To determine the type of license that NNM iSPI NET is using, do one of the following:

- At the NNMi console login window, click **View Licensing Information**.

- If you are already logged in to the NNMi console, click **Help** > **About Network Node Manager i-Series**. In the About Network Node Manager i-Series window, click **View Licensing Information**.

Obtaining and Installing a Permanent License Password

To obtain and install a permanent license password for NNM iSPI NET on the NNMi system, use the NNMi `nnmlicense.ovpl` tool.

Before requesting a permanent license password, gather the following information:

- The Entitlement Certificate, which contains the HP product number and order number

- The IP address of the NNMi management server

- Your company or organization information

Then follow these steps:

1 At a command prompt on the NNMi system, enter the following:

```
<drive>:\Program Files (x86)\HP\HP BTO
Software\bin\nnmlicense.ovpl iSPI-NET -g
```

> The product license ID (iSPI-NET) is case-sensitive.

2   In the **License Password** dialog box, click **Request License**.

3   Follow the instructions on the screen to obtain the permanent license
    password.

4   At a command prompt on the NNMi system, enter the following command
    to update the system and to store license data files:

```
<drive>:\Program Files (x86)\HP\HP BTO
Software\bin\nnmlicense.ovpl iSPI-NET -f <license_file>
```

> The product license ID (iSPI-NET) is case-sensitive.

Obtain Additional License Passwords

The capacity provided by your NNM iSPI NET licenses should match the
capacity of your NNMi licenses. In this case, *capacity* refers to the number of
nodes that the product is licensed to manage. If NNMi licensed capacity
exceeds NNM iSPI NET licensed capacity, you need to obtain additional NNM
iSPI NET licenses.

Contact your HP Sales Representative or your Authorized Hewlett-Packard
Reseller for information about the NNMi and NNM iSPI NET licensing
structure and to learn how to add license tiers for enterprise installations.

To obtain additional license passwords, go to the HP password delivery
service:

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

Remove NNM iSPI NET

To remove NNM iSPI NET software, do the following:

- Remove NNM iSPI NET references from the NNMi Console.
- Disable execution of diagnostics flows triggered by NNMi incidents.
- Remove the diagnostics flows and server.

Removing NNM iSPI NET References

If NNM iSPI NET is unlicensed, you can remove references to it from the NNMi Console; follow these steps:

> ⚠️ The steps below remove all menu items, views and workspaces for any unlicensed function, including NNMi Advanced and other NNM iSPIs if they are also unlicensed.

1 Log in to the NNMi Console as an administrator.

2 Click **Configuration** in the **Workspaces** navigation pane.

3 Click **User Interface Configuration…**

4 Uncheck the box next to **Show Unlicensed Features**.

5 Click **Save and Close**.

To remove an NNM iSPI NET license password (making NNM iSPI NET unlicensed), follow these steps:

1 At a command prompt on the NNMi system, enter the following:

    <drive>:\Program Files (x86)\HP\HP BTO
    Software\bin\nnmlicense.ovpl iSPI-NET -g

> ▶ The product license ID (iSPI-NET) is case-sensitive.

2 In the **License Password** dialog box, click **Remove License Key**.

Removing the Diagnostics Flows and Server

The NNM iSPI NET diagnostics server is an embedded HP Operations Orchestration Central with restricted capabilities. Follow these steps to unlink and remove the embedded HP OO Central server and the NNM iSPI NET diagnostics flows:

1   Make sure that all HP OO Central users log off.

2   Disable triggering of diagnostics flows on the NNMi server as follows:

   • Log in as an administrator to the system where NNMi is installed.

   • Bring up a command prompt and navigate to the support directory:

      Windows: `<drive>:\Program Files (x86)\HP\HP BTO Software\support\`

      Unix: `/opt/OV/support/`

   • Run the script `nnmdiagnostics.ovpl` with the `uninstall` command parameter:

      `nnmdiagnostics.ovpl uninstall`

3   Remove the embedded diagnostics server as follows:

   • Log in as an administrator to the system where the diagnostics server is installed.

   • Stop the services of the embedded HP Operations Orchestration Central: **RSCentral**, **RSJRAS**, and **RSScheduler**.

   • Open the Control Panel; then click **Add or Remove Programs**.

   • Remove **HP Operations Orchestration Central 7.20**.

   • (Optional) If the embedded HP OO Central is the only application using MySQL Server 5.0, remove **MySQL Server 5.0**.

   • Remove the directories where HP Operations Orchestration Central has been installed, typically:

      `<drive>:\Program Files (x86)\Hewlett-Packard\Operations Orchestration`

   • (Optional) Remove the directories where MySQL Server 5.0 has been installed, typically:

      `<drive>:\Program Files (x86)\MySQL\MySQL Server 5.0`

Disable NNMi Triggering of Diagnostics Flows

You might want to disable NNMi triggering of diagnostics flows without removing the server running those flows. For example, this can happen when you are running the NNM iSPI NET diagnostics flows using a full HP Operations Orchestration Central server rather than the embedded diagnostics server.

Disabling Diagnostics Flows

To shut down NNMi's automatic triggering of the diagnostics flows, follow these steps:

1 Log in as an administrator to the system where NNMi is installed.

2 Bring up a command prompt and navigate to the support directory:

   Windows: `<drive>:\Program Files (x86)\HP\HP BTO Software\support\`

   Unix: `/opt/OV/support/`

3 Run the script `nnmdiagnostics.ovpl` with the `uninstall` command parameter:

   `nnmdiagnostics.ovpl uninstall`

   > The `nnmdiagnostics.ovpl` script can also be used to do the following:
   >
   > • Determine the current HP OO Central server configuration:
   >
   >   `nnmdiagnostics.ovpl servers`
   >
   > • Change the password NNMi uses for the **admin** account on the HP OO Central server:
   >
   >   `nnmdiagnostics.ovpl credentials`
   >
   >   This is necessary if the **admin** account password changes on the HP OO Central server (whether the embedded diagnostics server or an existing HP OO Central server). If the password is changed on the HP OO Central side, NNMi needs to be informed of the change. You use `nnmdiagnostics.ovpl credentials` to provide NNMi with the new password.

Re-Enabling Diagnostics Flows

You can re-enable the triggering of the diagnostics flows by running the installer on the diagnostics server or on the HP Operations Orchestration Central server. For more information, see one of the following:

- Installing NNM iSPI NET Diagnostics on a System Without a Pre-existing HP Operations Orchestration Central on page 24.

- Installing the NNM iSPI NET Diagnostic Flows on an Existing HP Operations Orchestration Central Server on page 29.

The installer detects that the needed software is already installed and simply perform the configuration steps.

4 About NNM iSPI NET Components

This chapter provides information to help you begin using NNM iSPI NET tools.

Use the NNMi Console Help

Help for the NNM iSPI NET tools and commands is included with NNMi help, accessible from the NNMi console. Refer to the NNMi help for more details on specific tools and commands.

NNM iSPI NET Diagnostics

NNM iSPI NET Diagnostics (Flows) are sets of automated commands specific to one or more device type. You associate these diagnostics with incident configurations, including the associated Node Group and Lifecycle State.

After they are configured, diagnostics are automatically triggered by specific incidents. Diagnostics flow results are listed under the **Diagnostics** tab of the **Incident** form; they can be viewed in order to troubleshoot the problem on the source node.

Examples of the kinds of diagnostics that NNMi provides include the following:

- Determine the current configuration of a Cisco router, Cisco switch, or Nortel switch.

- Perform diagnostic checks on a specified interface on a Cisco router.

- Obtain routing information using the `show ip route` command.

- Determine failures of either a `ping` or `traceroute` to a target node.

- Determine statistics for a specified port on a Nortel switch.

- Load custom attributes onto nodes (such as location, service type, or asset number) using a comma separated values (CSV) file.

Configuring NNM iSPI NET Diagnostics

You use a two-step process to configure NNM iSPI NET to automatically gather diagnostic information about the source node whenever an incident reaches the lifecycle state you selected.

From the NNMi **SNMP Trap Configuration**, **Remote NNM 6.x/7.x Event Configuration** or **Management Event Configuration** forms:

1   Specify the Node Group using the **Configuration Per Node Group** form.

2   Specify the Diagnostics using the **Diagnostic Selection** form.

The **Configuration per Node Group** form enables you to specify the Node Group for which you want to automatically gather diagnostic information.

The **Diagnostic Selection** form enables you to specify the diagnostics you want NNMi to run on each applicable Source Node in the Node Group for the incident you are configuring.

After you configure the diagnostic for the incident and node group, the following criteria must be met before the diagnostic runs:

- The Source Node must be in the Node Group you have selected.

- The Diagnostic must be valid for the Source Node. (For example, only Nortel switch diagnostics are run on Nortel switches.)

- The incident's current lifecycle state must match a lifecycle state for which it was configured. (For example, if you configure the Incident to run a specified Diagnostic when the incident is Closed, then if the current Incident's Lifecycle State is Closed, NNMi runs that Diagnostic.)

- The Source Node must have device credentials set up in NNMi. See NNMi Management Server Preparation on page 13.

If these criteria are met, NNM iSPI NET runs the diagnostics and generates diagnostic reports to help you solve the problem on the source node.

> If NNMi has incorrect device credentials for the source node, the diagnostic report shows a device communication problem rather than the results of the diagnostic flow.

You can also run Diagnostics to access the Diagnostics reports on demand, using **Actions** > **Run Diagnostics** from the associated incident or node form.

In addition, NNM iSPI NET associates diagnostics with the node on which the diagnostic was run. To view the diagnostics automatically invoked for the node, open the **Node** form for any node of interest.

NNM iSPI NET SNMP Trap Analytics

By default, NNMi measures the rate of incoming traps, including the following:

- The rate of incoming SNMP traps from each device
- The rate of each incoming trap for each trap object identifier (OID)

NNMi monitors this trap information to determine whether any incoming traps exceed the configured threshold. If a threshold is exceeded, NNMi blocks the traps until the number of traps falls below the minimum threshold. The NNMi administrator can configure the threshold value using the nnmtrapconfig.ovpl script.

NNM iSPI NET SNMP Trap Analytics enables you to obtain reports about this trap information according to the following criteria:

- Within a specific time period
- For a specific node
- According to a specific trap identifier (trap OID)

When analyzing traps, NNMi looks at both the most common traps, as well as the most common source nodes from which the traps are received. This SNMP trap analytics data is logged to the trapanalytics.0.0.log file.

Information in the log file is organized as follows for specific time intervals:

- Trap rate in number of traps per second

- The top 10 addresses that are generating traps
- The top 10 traps that are being generated

To make this data more easily available, use the `nnmtrapdump.ovpl` command. This tool enables you to extract the data you are most interested in from the `trapanalytics.0.0.log` file.

See the `nnmtrapdump.ovpl` Reference Page for more information, including more details on the `trapanalytics.0.0.log` file and its location.

NNM iSPI NET Attached Switch Port Troubleshooting Tool

As part of the investigation and diagnosis process, you may need to determine the switch to which a problem node is connected. For example, if a node in your network has a potential virus, you want to identify the switch to which it is connected so that you can prevent the virus from moving to other nodes in your network.

The NNM iSPI NET Attached Switch Port Troubleshooting Tool enables you to identify a switch port attached to a problem node using the **Tools** > **Find Attached Switch Port** option from the NNMi console.

You can find the attached switch and the port that is connected from the switch to the problem node by specifying the fully-qualified DNS name of the problem node, or the IP or MAC address of any interface on it.

> ▶ The node whose information you provide (the problem node) does not have to be discovered by NNMi. However, the switch to which the problem node is attached does need to have been discovered by NNMi.

NNMi searches the database to find a matching value using the hostname, IP address, or MAC address provided.

NNMi shows the hostname of the node and the name of the node's interface or port number. Click the node name to open the **Node** form for the switch attached to the node you specified. Click the interface name to open the

Interface form. If the node or attached switch port is not found, NNMi shows an error message. If multiple attached switches are found, NNMi shows the first attached switch it finds.

See the NNMi console's **Help for Operators** for more information.

NNM iSPI NET Show Attached End Nodes Troubleshooting Tool

As you manage your network, you may need to determine the end nodes connected to a specified switch. For example, if you need to replace a switch, you may want to know which end nodes will be affected while the switch is out of service. The NNM iSPI NET **Show Attached End Nodes** tool uses information from the switch itself to report the end nodes attached to it.

> The attached end nodes do not have to be discovered by NNMi; however, NNMi must have discovered the switch itself.

To access this tool, navigate to the view or form of interest and select the switch whose attached end nodes you want to display. Then use the **Actions** > **Show Attached End Nodes** option from the NNMi console.

You can obtain more information about the results displayed by clicking any object name link to open the form for the selected object.

See the NNMi console's **Help for Operators** for more information.

NNM iSPI NET Load Custom Attributes on Nodes Command

You use the `nnmnetloadnodeattrs` command to load custom node attributes into NNMi from a comma separated values (CSV) file, such as a Microsoft® Excel spreadsheet. This command is useful if you have nodes with custom attributes defined in an external datastore.

After loading nodes with custom attributes into NNMi, you use the NNMi console or the `nnmloadnodegroups` command to group nodes according to their attributes.

▶ For more information about creating node groups, refer to the `nnmloadnodegroups` man page or reference page. Or go to the NNMi Console help.

Provide a CSV file

To load custom node attributes, the CSV file you supply must contain the following:

- Node DNS or IP address
- Attribute name
- Attribute value

You can specify each attribute name/attribute value pair on a separate line; for example:

192.168.2.2,Location,Fort Collins

192.168.2.2,Service Type,IT

192.168.2.2,Asset Tracking,N1234

Or you can specify a string of attribute name/value pairs on a single line; for example:

```
192.168.2.2,Location,Fort Collins,Service Type,IT,Asset
Tracking,N1234
```

> ▶ You can use Microsoft Excel to create comma separated (CSV) files, but .csv files do not maintain the Excel spreadsheet's column width, comments, and other features.
>
> To maintain these features, store the nnmnetloadnodeattrs.ovpl input file in an Excel .xls format. Then select **File** > **Save As...** to create a .csv file.

Load Custom Node Attributes Command

The nnmnetloadnodeattrs.ovpl command is in the NNMi bin directory. For command syntax, refer to the nnmnetloadnodeattrs man page or reference page.

Delete Custom Node Attributes Command

The nnmnetdeletenodeattrs.ovpl command is in the NNMi bin directory. For command syntax, refer to the nnmnetdeletenodeattrs man page or reference page.

5 Troubleshooting Installation and Initial Startup

Installation Problems

If you encounter errors during installation of the NNM iSPI NET diagnostics server, you first see the error in an error message pop-up. Once you close the pop-up, you return to the Installer Welcome window with the error message displayed in the text box. Finally, error messages are logged to the installer log.

The installer log is named `nnm-ispi-net-server-installer.log`, and it is created in the temporary files directory for the user doing the install. For the user **Administrator**, this file will typically be in `C:\Documents and Settings\Administrator\Local Settings\Temp`

You can restart the installation without having to close the Installer window. If you click **Start Over** to restart the installation, the **Configuration Parameters** dialog is populated with the values you previously specified. This can be helpful if you have specified an incorrect user name or password for one of the components, or an HTTP or HTTPS port that is already in use. You can leave all the other parameters as originally specified and change only the problem parameter. However, you need to be aware that these configuration parameters do not persist once you exit the installer. If you exit the installer and then run it, you need to type the configuration parameters again.

Problem: Diagnostics server installation subprocesses do not terminate immediately when installation is cancelled

Solution:

If you click **Quit** in the main server Installer window, the .NET and HP Operations Orchestration installation subprocesses run to completion once they are initiated as part of the install. The MySQL installation subprocess can be canceled from the MySQL Installer window.

Problem: Cannot create database or add user during MySQL configuration

Solution:

If you are using the embedded HP OO Central diagnostics server:

- During MySQL configuration, you may have specified a different password for the MySQL root account than the password specified in the NNM iSPI NET server installer Configuration Parameters window. To verify the password for the MySQL root account:

  — At a command prompt, navigate to the bin directory under the MySQL install directory (typically, C:\Program Files (x86)\MySQL\MySQL Server 5.0\bin\).

  — Enter the following command:

    mysql -u root -p

  — At the password prompt, enter the same password for MySQL user root that you entered in the NNM iSPI NET server installer Configuration Parameters window.

  — If the password is correct, you see a mysql> prompt. If the password is incorrect, you see an Access Denied error.

  Once you have determined the correct password, either use **Start Over** in the NNM iSPI NET server installer or run the installer again.

If you are using an existing MySQL server:

- Verify that you have the correct root user name and password. Change these values in the Configuration Parameters window, if necessary.

- If the existing MySQL database is on a remote system, verify that you can login remotely to the root user account. If necessary, enable remote login for the duration of the MySQL configuration step.

- Verify that your database and database user names do not conflict with names already in use on this MySQL server. Change these values in the Configuration Parameters window, if necessary.

Once you've corrected any problems, click **Start Over** in the diagnostics server installer to try the MySQL configuration step again.

Problem: Diagnostics server installer reports an NNMi binding failure

This can occur if you incorrectly specify one or more of the NNMi fields in the Configuration Parameters step of NNM iSPI NET server installation.

Solution:

To check that you have the correct values in these fields:

- Open a browser and navigate to **http://<*hostname*>:<*port*>/nnm**, where <*hostname*> is the value you specified during installation for the NNMi **Hostname or IP Address** and <*port*> is the value you specified during installation for the NNMi **HTTP Port**.

- Log in as the user you specified for the NNMi **Administrative Username**, using the password you specified during installation for the NNMi **Administrative Password**.

Once you have verified the NNMi server's hostname, port, administrative user account, and administrative user password, either use **Start Over** in the NNM iSPI NET server installer or run the installer again.

If you are using an existing HP OO Central server, verify that you have created the required certificate files as described under Creating Certificate Files on an Existing HP OO Central Server on page 16.

Execution Problems

Messages related to diagnostic flow execution are logged to the following files on the NNMi server. Check these log files for error messages if you encounter diagnostic submittal problems on the NNMi server.

Windows:

```
C:\Documents and Settings\All Users\Application Data\HP\HP
BTO Software\log\nnm\rba.%g.%u.log
```

Unix:

```
/var/opt/OV/log/nnm/rba.%g.%u.log
```

where

%g = Zero (0) for active log files. Any other number means an archived log file from previous restarts or from reaching log file size limits.

%u = Zero (0) unless the service failed to obtain a lock on the log file during a logging session.

Problem: Diagnostic flows are listed as "Not Submitted"

If the flows displayed under the **Diagnostics** tab of a Node or Incident form are classified as "Not Submitted," NNMi may be unable to find device credentials for the target node, or the HP Operations Orchestration Central SSL certificates may be incorrect.

Solution:

Check `rba.0.0.log` (or older log file) on the NNMi server for error messages from the same timeframe as the failing flows.

If the error messages indicate that a password or login information is missing, use the **Communication Configuration** form in the **Configuration** workspace of the NNMi console to create **Default Device Credentials**. Then use **Regions** and **Specific Node Settings** to provide any device credentials that differ from the defaults.

If the error messages indicate a missing hostname or other communication issue with the HP OO Central server, check to make sure that the SSL certificates have been set up on the HP OO Central server as described in Creating Certificate Files on an Existing HP OO Central Server on page 16.

Problem: Diagnostic flow results report a communication problem with the device

This indicates that NNMi has the wrong device credentials for this device.

Solution:

You can use **Telnet... (from client)** from a topology map or the Node form for the device to check whether the device credentials are correct. (Or, use **ssh** to log in to the device.)

Once you have verified that you have the correct username and password, correct or add the appropriate setting using the **Default Device Credentials**, **Regions**, or **Specific Node Settings** tab in the **Communication Configuration** form in the NNMi console Configuration workspace.

Problem: NNMi reports 0 diagnostic flows submitted

This problem indicates that you have attempted to run a diagnostics flow for a device which has no associated flows.

Solution:

Only certain types of devices have associated diagnostics flows. See the HP NNM iSPI NET Software System and Device Support Matrix for details about supported devices.

Problem: NNMi does not use credentials supplied in Specific Node Settings

NNMi might not find the correct device credentials if you use an IP address or a hostname that is not fully qualified in **Specific Node Settings**.

Solution:

If NNMi found a fully qualified domain name for a node during discovery, this name must be used to identify the node in **Specific Node Settings**. For example, suppose NNMi discovery processes have identified the node by its fully qualified domain name:

> `rtr17.bldg3.acompany.com`

You cannot use **rtr17** or an IP address to identify the node in **Specific Node Settings**. You must use **rtr17.bldg3.acompany.com**. An IP address can be used only if NNMi does not have a fully qualified domain name for the node.

To determine how NNMi has identified a node, open a Node form for the node from a topology map or a table view. The **Hostname** value in the Node form contains a fully qualified domain name or an IP address, depending on what NNMi found during discovery. Use the value from the **Hostname** field to identify the node in **Specific Node Settings**.

Index