HP NNM iSPI Network Engineering Toolset Software

for the Windows® operating system

Software Version: 9.00

Planning and Installation Guide

Manufacturing Part Number: TB775-90000
Document Release Date: March 2010
Software Release Date: March 2010

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2008–2010 Hewlett-Packard Development Company, L.P.

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.

This product includes Commons Discovery software developed by the Apache Software Foundation (http://www.apache.org/). Copyright © 2002-2008 The Apache Software Foundation. All Rights Reserved.

This product includes Netscape JavaScript Browser Detection Library software, Copyright © Netscape Communications 1999-2001

This product includes Xerces-J xml parser software developed by the Apache Software Foundation (http://www.apache.org/). Copyright © 1999-2002 The Apache Software Foundation. All rights reserved.

This product includes software developed by the Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). Xpp-3 Copyright © 2002 Extreme! Lab, Indiana University. All rights reserved.

Trademark Notices

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 U.S. trademark of Sun Microsystems, Inc.

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

MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries.

UNIX® is a registered trademark of The Open Group.

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 sign-in 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	9.00	Second publication

Support

You can 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 Software 7
How is NNM iSPI NET Installed? 8
How is NNM iSPI NET Licensed? 8

2 Preinstallation Checklists 9
Supported Hardware and Software 9
NNMi Management Server Preparation 11
Diagnostics Server System Preparation 12
Creating Certificate Files on an Existing HP OO Central Server 14

3 Installing the NNM iSPI NET Diagnostics Server and Diagnostic Flows 19
Upgrade NNM iSPI NET 20
Install NNM iSPI NET 20
Installing NNM iSPI NET Diagnostics on a System Without a Pre-existing HP OO Central 20
Installing the NNM iSPI NET Diagnostic Flows on an Existing HP OO Central Server 25
Creating Users on the Diagnostics Server 29
Setting Up Diagnostics Server User Accounts 29
License NNM iSPI NET 30
Checking the License Type 30
Obtaining and Installing a Permanent License Key 30
Obtain Additional License Keys 31
Disable NNMi Triggering of Diagnostic Flows 32
Disabling Diagnostic Flows 32
Re-Enabling Diagnostic Flows 33
Remove NNM iSPI NET 33

4 About NNM iSPI NET Components 37
NNM iSPI NET Diagnostics 37
Configuring NNM iSPI NET Diagnostics 38
Using NNM iSPI NET Diagnostics 38
NNM iSPI NET SNMP Trap Analytics 39
NNM iSPI NET Visio Export Functionality 40
5 Troubleshooting Installation and Runtime Problems 41
Diagnostics Server Installation Problems 41
Diagnostic Flows Runtime Problems 43
Visio Export Functionality Problems 46
Index 49

1 Introducing HP NNM iSPI Network Engineering Toolset Software

The HP NNM iSPI Network Engineering Toolset Software (NNM iSPI NET) extends the powerful network management capabilities of NNMi by providing additional troubleshooting and diagnostic tools for network engineers. Purchasing NNM iSPI NET provides the following functionality:

- NNM iSPI NET functionality in the NNMi console (enabled with an NNM iSPI NET license):
  - SNMP trap analytics provide summary and detailed information about SNMP trap traffic in the network.
  - Visio export functionality exports NNMi topology map data to Microsoft Visio files.
  - If the HP Network Automation Software integration with NNMi is enabled, the **Show mismatched connections** menu item displays a table of all layer 2 connections with possible speed or duplex configuration differences. For more information, see the "HP Network Automation" chapter in *NNMi Deployment Reference*.

    For information about the supported hardware, operating systems, and web browsers for the NNMi console, see the *NNMi System and Device Support Matrix*.

- NNM iSPI NET diagnostic flows and diagnostics server, which must be installed separately from NNMi (on the NNMi management server or on a separate computer):
  - The diagnostic flows automatically gather diagnostic information when NNMi detects certain network incidents.

— The diagnostics server is an embedded packaging of HP Operations Orchestration (HP OO). If you already have the full HP OO product, you can install the NNM iSPI NET diagnostic flows on that server.

For information about the supported hardware, operating systems, and web browsers for the embedded diagnostics server as well as information about the supported versions of the full HP OO product, see the *NNM iSPI NET Diagnostics Server System and Device Support Matrix*.

How is NNM iSPI NET Installed?

The NNM iSPI NET SNMP trap analytics and Visio export functionality are automatically installed with NNMi. The diagnostic flows and diagnostics server must be installed from a separate installation media. See Chapter 3, Installing the NNM iSPI NET Diagnostics Server and Diagnostic Flows for details.

How is NNM iSPI NET Licensed?

When you install NNMi, the NNM iSPI NET functionality is enabled with a temporary Instant-On license key. Purchase a permanent NNM iSPI NET license separately from your permanent NNMi license. See License NNM iSPI NET on page 30 for details.

2 Preinstallation 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 the Visio export functionality 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 the NNM iSPI NET diagnostics, read the information about supported hardware and software described in Table 1.

For the most current versions of all documents listed here, go to the following web site:

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

Table 1 Software and Hardware Preinstallation Checklist

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

HP updates the *NNM iSPI NET Diagnostics Server System and Device Support Matrix* as new information becomes available. Before you begin to install the NNM iSPI NET diagnostics server, check for the most recent NNM iSPI NET 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

In a diagnostic flow, the first step is to log on to the device. NNM iSPI NET uses the device credentials that NNMi stores. 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 some devices have 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 diagnostic flows will be run. See the *NNM iSPI NET Diagnostics Server System and Device Support Matrix* for details about supported devices.

Diagnostics Server System Preparation

The NNM iSPI NET diagnostics server includes an embedded version of HP Operations Orchestration (HP OO) Central with restricted capabilities. The NNM iSPI NET diagnostic flows can be run by this embedded diagnostics server or by an HP OO 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 system that has sufficient resources and is running the correct operating system version.

For information about the supported hardware, operating systems, and web browsers for the embedded diagnostics server as well as information about the supported versions of the full HP OO product, see the *NNM iSPI NET Diagnostics Server System and Device Support Matrix*.

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 OO Central already installed in your environment, gather the following information: • The HTTP and HTTPS port numbers used by HP OO Central • The password for HP OO Central `admin` user
	If you plan to use an HP OO Central already installed in your environment, you must create new certificate files so the installer can install diagnostic flows. See Creating Certificate Files on an Existing HP OO Central Server on page 14.

Table 2 Diagnostics Server Preparation Checklist (cont'd)

Complete (y/n)	Diagnostics Server Preparation
	The NNM iSPI NET diagnostics server requires MySQL. The NNM iSPI NET diagnostics 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 files are typically 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, gather the following information: • 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 MySQL database (this database cannot already exist—it will be created during the installation) • A database user name and password for accessing the MySQL database on the diagnostics server If the existing MySQL server is installed on a separate system from the NNM iSPI NET diagnostics server, the MySQL server must permit remote access for the database `root` user.
	Gather the following NNMi information: • The hostname or IP address of the NNMi management server • The port of the NNMi management server • The password for the NNMi `system` user
	The NNM iSPI NET diagnostics server installer requires an HTTP connection to the NNMi management server. Verify that this access is available.

Table 2 Diagnostics Server Preparation Checklist (cont'd)

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 that NNMi can identify this hostname as the diagnostic server hostname, follow these steps: 1 Log on to the NNMi management server. 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 *NNM iSPI NET Diagnostics Server System and Device Support Matrix*.

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 diagnostic flows, you must create an SSL certificate file for the NNM iSPI NET diagnostics server installer. The installer looks for this file in a specific location. You must create the file before installing the NNM iSPI NET diagnostic flows.

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

If you have note 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 server might 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:

- Task 1: Set Environment Variables in a command window on the HP OO Central server. Complete the remaining tasks in this command window.
- Task 2: Check the SSL Certificate to determine whether the current HP OO Central keystore entry contains a valid hostname.
- Task 3: Replace the 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.

- Task 4: Create the Certificate File used by the NNM iSPI NET diagnostics server installer.

Task 1: Set Environment Variables

The example commands in this section use environment variables. Set these environment variables as follows:

1 Log on with administrator privileges to the HP OO Central server and open a command window.

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

```
echo %ICONCLUDE_HOME%
```

The output should be 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.example.com>
```

Use the current system hostname for ***<server.example.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 hostname, follow these steps:

1 Log on to the NNMi management server.
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 the HP OO Central keystore entries for hostname as follows:

1 Enter the following Java *keytool* command:

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

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

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

- If the *keyEntry* does not include the hostname of the HP OO Central server, you must replace it. Continue with Task 3: Replace the Keystore Entry.
- 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. Continue with Task 4: Create the Certificate File.

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 hostname, see the command for setting `%HOSTNAME%` in step 3 on page 16.

Task 3: Replace the Keystore Entry

The NNMi 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%` in step 3 on page 16.

- NNMi does not communicate directly with the HP OO RAS service, which means that you can leave the 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 might 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, and 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 diagnostics server installer. Continue with Task 4: Create the Certificate File.

Task 4: Create the Certificate File

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

Export the `%PAS_KEYSTORE%` entry to its certificate file by entering 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 Task 2: Check the SSL Certificate.

After you create the `nnmgenpas.cer` file, you can run the NNM iSPI NET diagnostics server installer. See Chapter 3, Installing the NNM iSPI NET Diagnostics Server and Diagnostic Flows.

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

3 Installing the NNM iSPI NET Diagnostics Server and Diagnostic Flows

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 (HP OO) Central with restricted capabilities. NNM iSPI NET diagnostic flows can be run by this diagnostics server or by an HP OO Central server already installed in your environment.

If NNMi is installed on a system that has sufficient resources and is running the correct operating system version, you can install the embedded NNM iSPI NET diagnostics server on the same system. (See Chapter 2, Preinstallation Checklists.)

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

- If HP OO Central is not installed on the system, the NNM iSPI NET diagnostics 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 management server.
- If HP OO Central is already installed, the NNM iSPI NET diagnostics server installer installs the NNM iSPI NET diagnostic flows and sets up the binding between HP OO Central and the NNMi management server.

Before you begin, complete the requirements in Chapter 2, Preinstallation Checklists.

Upgrade NNM iSPI NET

NNM iSPI NET version 9.00 enables new functionality in the NNMi console.

If the NNM iSPI NET diagnostic flows are running correctly in an NNMi 8.1x environment, you do not need to install the NNM iSPI NET diagnostics server software provided with NNM iSPI NET version 9.00, nor do you need to change the HP OO configuration.

Install NNM iSPI NET

To install NNM iSPI NET, first install NNMi as described in the *NNMi Installation Guide*. This installation provides the SNMP trap analytics and the Visio export functionality. Then, install the NNM iSPI NET diagnostics server and diagnostic flows.

The NNM iSPI NET diagnostics server installer requires an HTTP connection to the NNMi management server.

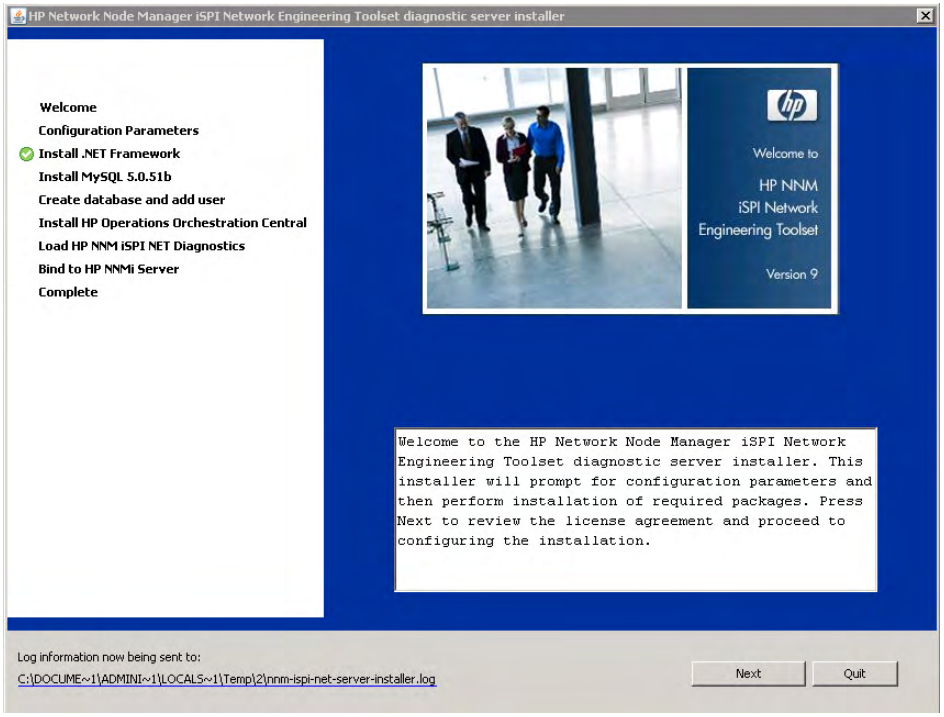
Installing NNM iSPI NET Diagnostics on a System Without a Pre-existing HP OO Central

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

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

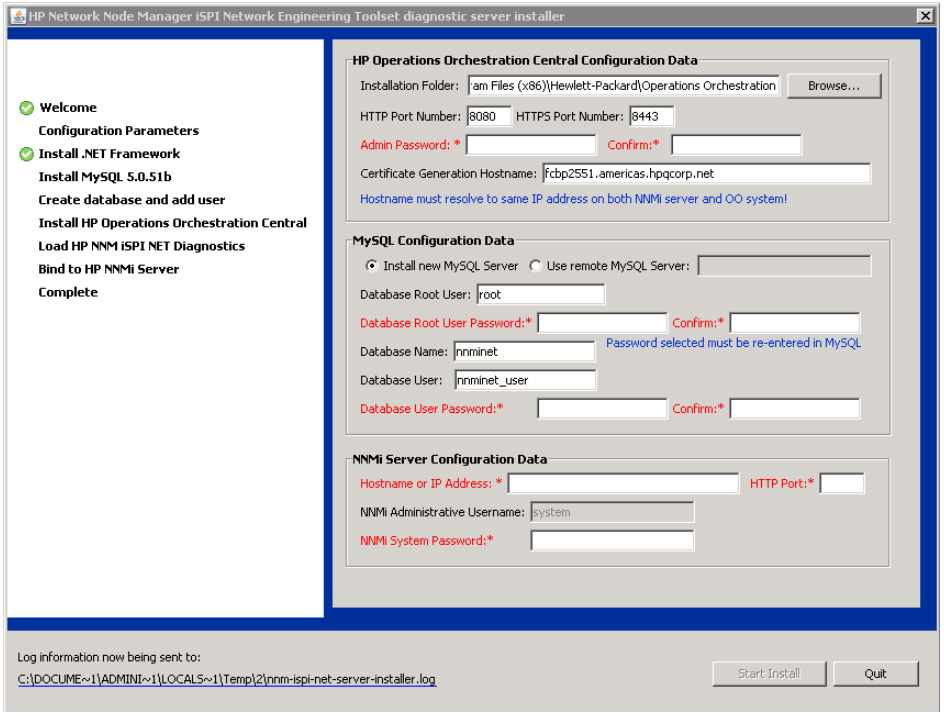
The installer Welcome window lists the installation steps. These steps are described in this procedure.

If components such as .NET or MySQL are already installed, a check mark indicates that these installation steps are complete.



4 Click **Next**, and then accept the license agreement.

The Configuration Parameters window appears, as shown here.



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. After valid data has been entered, the asterisk disappears and the label text turns black.
- The **HP Operations Orchestration Central Configuration Data** items refer to the diagnostics server. This server is an embedded HP OO Central server. In this procedure, step 6 and step 7 provide the 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 OO Central.
- 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 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 logon 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 the steps in Table 2 on page 14.

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 Identify the NNMi management server as follows:

- Enter the hostname or IP address of the NNMi management server.
- Enter the HTTP port used by NNMi.
- Enter the password for the NNMi `system` user.

9 After 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 installation log file at any time during the installation by clicking 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 diagnostics 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 diagnostics server installer window after MySQL configuration is finished. This manual step ensures that MySQL is active before the NNM iSPI NET diagnostics server installer accesses it.

12 The remaining steps of the NNM iSPI NET diagnostics server installation complete automatically:

- Installing the embedded HP OO Central server
- Loading the NNM iSPI NET diagnostic flows
- Binding to the NNMi management server

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

After all installation steps have completed, a completion message appears in the installer window and **Finish** becomes active.

By default, the embedded HP OO Central user interface opens when you click **Finish**. To skip this launch, clear the **Launch HP OO** check box.

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

If you chose to launch the embedded HP OO Central user interface, your browser opens.

You might 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. You can safely ignore this warning.

Installing the NNM iSPI NET Diagnostic Flows on an Existing HP OO Central Server

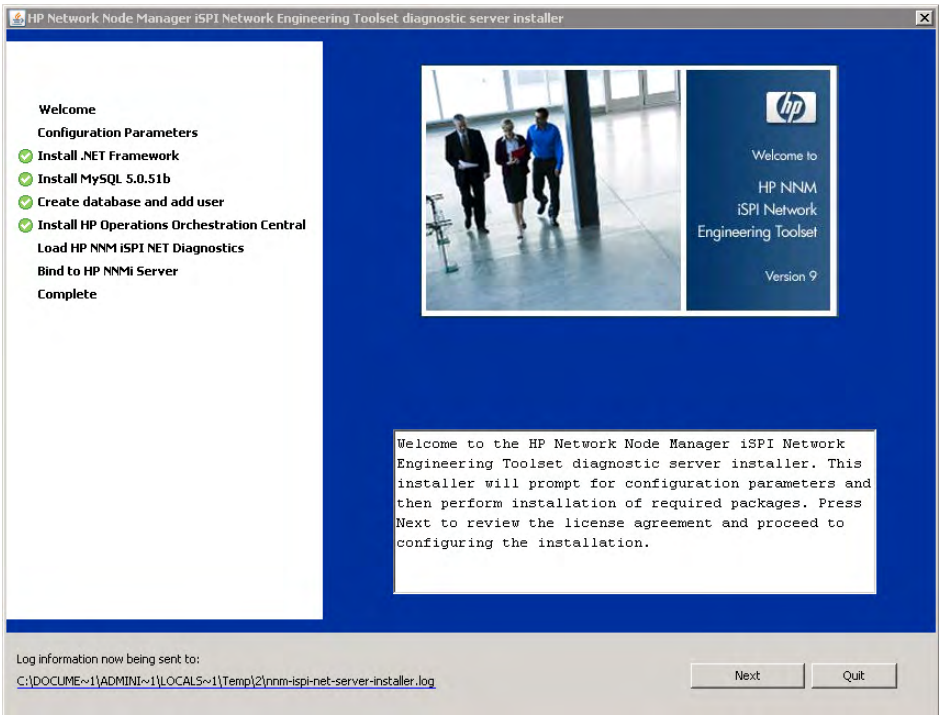
1 Log on with administrator privileges to the system running the existing HP OO Central.

2 Insert the NNM iSPI NET 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.

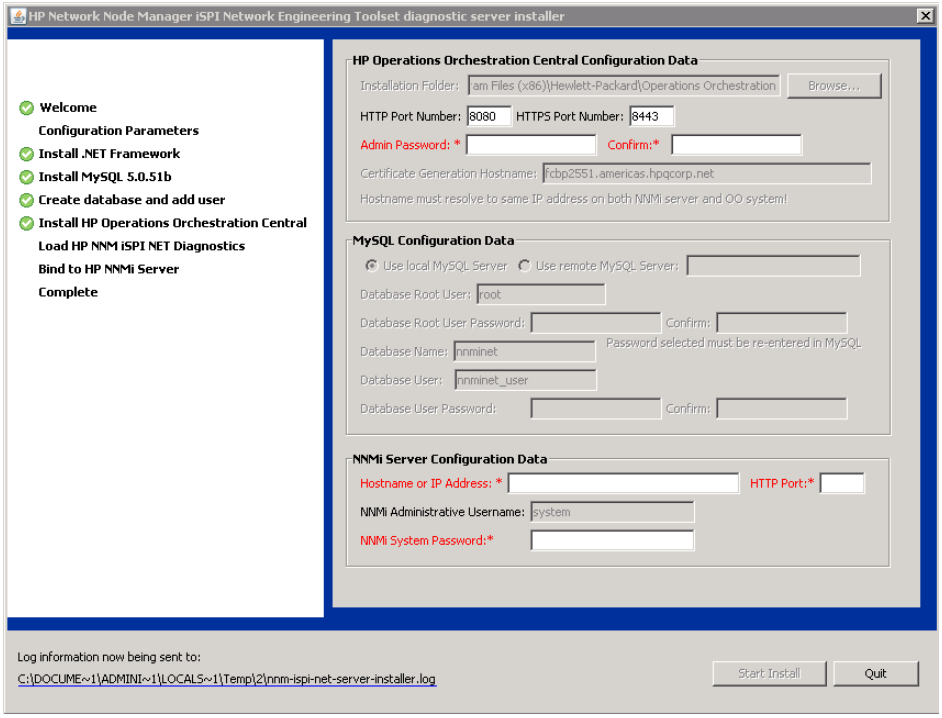
The installer Welcome window lists the installation steps. These steps are described in this procedure.

Because HP OO Central is already installed on this system, check marks indicate the installation steps that have already been completed.



4 Click **Next**, and then accept the license agreement.

The Configuration Parameters window appears, as shown here.



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. After valid data has been entered, the asterisk disappears and the label text turns black.
- Because HP OO Central is already installed on this system, many of the configuration fields are not available.

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 password for the `system` user for the NNMi management server.

After 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 diagnostics server installer complete automatically:

- Loading the NNM iSPI NET diagnostic flows
- Binding to the NNMi management server

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

8 After all installation steps have completed, a completion message appears in the installer window and **Finish** becomes active.

By default, the HP OO Central user interface opens when you click **Finish**. To skip this launch, clear the **Launch HP OO** check box.

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

Creating Users on the Diagnostics Server

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

If you installed the diagnostic flows on a pre-existing HP OO 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. Open the diagnostics server logon page by entering the following URL into a web browser window:

   http://<*hostname*>:<*port*>/PAS/

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

2. Log on as **`admin`** using the password you specified during installation.
3. On the **Administration** tab, click **Manage Users**.
4. For each user account, do the following:
   a. Click **Add New User**.
   b. Enter a user account name.
   c. Select the **Internal Account** check box.
   d. Enter the account password in the **User Password** and **Verify Password** fields.
   e. Click **Create User**.

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

License NNM iSPI NET

When you install NNMi, the NNM iSPI NET functionality is enabled with a temporary Instant-On license key. Purchase a permanent NNM iSPI NET license separately from your permanent NNMi license. You should obtain and install a permanent license key as soon as possible.

Checking the License Type

To determine the type of license that NNM iSPI NET is using, in the NNMi console, click **Help > System Information**. In the System Information window, click **View Licensing Information**.

Obtaining and Installing a Permanent License Key

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

Before requesting a permanent license key, 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

After gathering the necessary information, follow these steps:

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

```
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 key.

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

```
nnmlicense.ovpl iSPI-NET -f <license_file>
```

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

Obtain Additional License Keys

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 keys, go to the HP password delivery service:

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

Disable NNMi Triggering of Diagnostic Flows

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

Disabling Diagnostic Flows

To stop NNMi from automatically triggering the diagnostic flows, follow these steps:

1. Log on as an administrator to the NNMi management server.
2. In a command window, navigate to the support directory:

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

   UNIX: `/opt/OV/support/`
3. Run the `nnmdiagnostics.ovpl` command with the `uninstall` option:

   ```
   nnmdiagnostics.ovpl uninstall
   ```

   The `nnmdiagnostics.ovpl` command can also 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
     ```

     If the `admin` account password changes on the HP OO Central server (whether the embedded diagnostics server or an existing HP OO Central server), NNMi needs to be informed of the change. Use `nnmdiagnostics.ovpl credentials` to provide NNMi with the new password.

Re-Enabling Diagnostic Flows

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

- Installing NNM iSPI NET Diagnostics on a System Without a Pre-existing HP OO Central on page 20.
- Installing the NNM iSPI NET Diagnostic Flows on an Existing HP OO Central Server on page 25.

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

Remove NNM iSPI NET

To remove the NNM iSPI NET software, do the following:

- Task 1: Remove NNM iSPI NET References from the NNMi Console
- Task 2: Disable the Triggering of Diagnostic Flows
- Task 3: Remove the Diagnostic Flows and Server

Task 1: Remove NNM iSPI NET References from the NNMi Console

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

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

1. Sign in to the NNMi console as an administrator.
2. Click **Configuration** in the **Workspaces** navigation pane.
3. Click **User Interface Configuration**.
4. Clear the **Show Unlicensed Features** check box.
5. Click **Save and Close**.

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

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

```
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**.

Task 2: Disable the Triggering of Diagnostic Flows

To disable the running of diagnostic flows triggered by NNMi incidents, follow these steps:

1 Log on as an administrator to the NNMi management server.

2 In a command window, navigate to the support directory:

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

UNIX: `/opt/OV/support/`

3 Run the `nnmdiagnostics.ovpl` command with the `uninstall` option:

```
nnmdiagnostics.ovpl uninstall
```

Task 3: Remove the Diagnostic Flows and Server

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

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

2 Remove the embedded diagnostics server as follows:

- Log on as an administrator to the system where the diagnostics server is installed.
- Stop the services of the embedded HP OO Central: **RSCentral**, **RSJRAS**, and **RSScheduler**.
- Open the Control Panel, and 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 OO 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
  ```

4 About NNM iSPI NET Components

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

NNM iSPI NET Diagnostics

NNM iSPI NET diagnostics (flows) are sets of automated commands specific to one or more device types. 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. Diagnostic flow results are listed under the **Diagnostics** tab of the **Incident** form. Flow results can help you troubleshoot the problem on the source node.

Examples of the kinds of diagnostics that NNM iSPI NET 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 tracing the route to a target node.
- Determine statistics for a specified port on a Nortel switch.

For information about the available diagnostics, see *Diagnostics (Flows) Provided by NNM iSPI NET* in the NNMi help.

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

1. On the **Node Settings** form, specify the node group for which you want to automatically gather diagnostic information.
2. On the **Diagnostic Selections** form, specify the diagnostics you want NNMi to run on each applicable source node in the node group for the incident you are configuring.

For more information, see *Configure Diagnostics for an Incident* in the NNMi help.

Using NNM iSPI NET Diagnostics

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

- 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, if the current incident's lifecycle state changes to Closed, NNMi runs that diagnostic.)
- Device credentials for the source node must be set up in NNMi. See NNMi Management Server Preparation on page 11.

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 run diagnostics on demand, using **Actions** > **Run Diagnostics** from the associated Node form. In this way, you can gather baseline information for a device before any problems occur. You can also use **Actions** > **Run Diagnostics** from an Incident 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.

For information about diagnostic results, see *Incident Diagnostic Results Form (Flow Run Result)* and *Node Diagnostic Results Form (Flow Run Result)* in the NNMi help.

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 rate threshold. If a threshold is exceeded, NNMi blocks the traps from the device (or for the specific trap OID) until the number of traps falls below the minimum rearm value. The NNMi administrator can configure the threshold and rearm values with the `nnmtrapconfig.ovpl` command. For more information, see the *nnmtrapconfig.ovpl* reference page, or the UNIX manpage.

NNM iSPI NET SNMP Trap Analytics provides 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

In the NNMi console, you can access the `trapanalytics.0.0.log` file with **Tools > Trap Analytics > Trap Analysis Log**. For information about individual traps that arrived in the time window mentioned in the analytics report, use the `nnmtrapdump.ovpl` command. For more information, including details on the `trapanalytics.0.0.log` file and its location, see the *nnmtrapdump.ovpl* reference page, or the UNIX manpage.

The **Tools > Trap Analytics** menu in the NNMi console provides access to trap analytics reports. From a report window, you can start graphs of the trap rate for one or more nodes or trap OIDs.

For more information about the NNM iSPI NET SNMP Trap Analytics reports, see *Analyze Trap Information* in the NNMi help.

NNM iSPI NET Visio Export Functionality

You can export the information from one or more NNMi topology maps to an XML formatted (.vdx) file that Visio can read. For example, you might want to export the Network Overview topology map before a major change to your network infrastructure. You can open this file in Visio, and you can share the file with people who do not use NNMi.

The **Tools > Visio Export > Current Map** command creates a Visio file containing one sheet that shows the topology of the map from which you invoke the command.

The **Tools > Visio Export > Saved Node Group Maps** command creates a Visio file containing one sheet per node group map. To include a node group map in this larger file, select the **Include in Visio Export** check box on the **Node Group Map Settings** form for the node group.

For more information about the Visio export functionality, including how you can modify and print the file within Visio, see *Export Maps to Microsoft Visio* in the NNMi help.

5 Troubleshooting Installation and Runtime Problems

Diagnostics Server Installation Problems

If you encounter errors during installation of the NNM iSPI NET diagnostics server, the error first appears in an error message window. After you close the message window, the installer Welcome window displays the error message in the text box. The NNM iSPI NET diagnostics server installer logs all error messages to the installation log.

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

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 specified previously. This restart 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 other parameters as originally specified and change only the problem parameter. However, be aware that these configuration parameters do not persist after 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 OO installation subprocesses run to completion after 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 might have specified a different password for the MySQL `root` account than the password specified in the NNM iSPI NET diagnostics 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 diagnostics 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.

  After you have determined the correct password, either click **Start Over** in the NNM iSPI NET diagnostics 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 log on remotely to the `root` user account. If necessary, enable remote logon 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.

After you have 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 problem can occur if you incorrectly specify one or more of the NNMi fields in the Configuration Parameters step of NNM iSPI NET diagnostics 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**.
- Sign in to NNMi as the `system` user using the password you specified during installation for the NNMi **Administrative Password**.

After you have verified the NNMi management server's hostname, port, and `system` user password, either click **Start Over** in the NNM iSPI NET diagnostics 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 14.

Diagnostic Flows Runtime Problems

Messages related to the running of diagnostic flows are logged to the `nnm.0.0.log` (and older) files on the NNMi management server. If you encounter diagnostic submittal problems on the NNMi management server, check these log files for SEVERE and WARNING messages for the `com.hp.ov.nms.rba` class.

The `nnm.0.0.log` file is in the following location:

- *Windows Server 2008*:

  ```
  C:\ProgramData\HP\HP BTO Software\log\nnm\nnm.%g.%u.log
  ```

- *Windows Server 2003*:

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

- *UNIX*:

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

For more information about NNMi logging, including the versioning of log files, see the *logging.properties* reference page, or the UNIX manpage.

Problem: Diagnostic flows are listed as "Not Submitted"

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

Solution:

Check the `nnm.0.0.log` file (or an older log file) on the NNMi management server for SEVERE or WARNING messages from the same time frame as the failing flows.

If the error messages indicate that a password or logon 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, verify 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 14.

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

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

Solution:

You can telnet or ssh to the device to check whether the device credentials are correct.

After 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 diagnostic flow for a device that has no associated flows.

Solution:

Only certain types of devices have associated diagnostic flows. See the *NNM iSPI NET Diagnostics Server System and Device Support Matrix* for details about supported devices.

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

If the **Target Hostname** field of the Specific Node Settings form does not exactly match the value of the node hostname attribute in the NNMi inventory, NNMi might not find the correct credentials for the device.

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.example.com
```

You cannot use `rtr17` or an IP address to identify the node in **Specific Node Settings**. You must use `rtr17.bldg3.example.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**.

Visio Export Functionality Problems

Messages related to Visio export are logged to the `nnm.0.0.log` (and older) files on the NNMi management server. If you experience problems with exporting maps to Visio, check these log files for SEVERE and WARNING messages for the following classes:

- `com.hp.ov.nms.ui.visio.*`
- `com.hp.ov.nms.ui.framework.web.servlets.VisioViewSerlvet`

The `nnm.0.0.log` file is in the following location:

- *Windows Server 2008*:

  `C:\ProgramData\HP\HP BTO Software\log\nnm\nnm.%g.%u.log`

- *Windows Server 2003*:

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

- *UNIX*:

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

For more information about NNMi logging, including the versioning of log files, see the *logging.properties* reference page, or the UNIX manpage.

Problem: Cannot open the Visio file directly from NNMi

If the File Download window does not include the Open button, Visio is not installed on the computer where the NNMi console is running.

Solution:

Install the correct version of Visio (as described in the *NNMi System and Device Support Matrix*) on the computer running the NNMi console. Alternatively, you can save the file to the NNMi management server and then move it to a different computer where the correct version of Visio is installed.

Problem: Visio file does not open correctly

The Visio installation might be an incorrect version or might be corrupted.

Solution:

Install the correct version of Visio (as described in the *NNMi System and Device Support Matrix*).

Problem: Node group map not exported with Saved Node Group Maps command

The node group might not be configured correctly.

Solution:

For each node group map you want to export with the Saved Node Group Maps command, verify that the **Include in Visio Export** check box is selected on the Node Group Map Settings form

Problem: Export is very slow

Each node on a map increases the export time.

Solution:

On the Node Group Map Settings form, reduce the values of the **Maximum Number of Displayed Nodes** and **Maximum Number of Displayed End Points** attributes.

Problem: Export file is too large

All information in the export increases the file size.

Solution:

In the Visio Map Export window, clear the **Include connection labels** check box. This configuration limits the amount of data exported for each connection, which results in a smaller file size.

Problem: No download window

One or both of the **Visio Map Export** and **File Download** windows do not open

Solution:

Check the `nnm.0.0.log` file (or an older log file) on the NNMi management server for SEVERE or WARNING messages.

Problem: Visio Export menu not enabled or gives Access Denied message

By default, the Visio export functionality requires the Operator 2 or Administrator role.

Solution:

Ask the NNMi administrator for a different role.

Index

Symbols

.vdx file format, 40

A

additional licenses, 31

C

checklists
- diagnostics server preparation, 12
- preinstallation, 9

commands
- nnmdiagnostics.ovpl, 32
- nnmtrapconfig.ovpl, 39
- nnmtrapdump.ovpl, 40

configuration parameters, 22, 27

D

device credentials, 11, 44

diagnostic flows, 37
- disable triggering from NNMi, 32, 34
- installing flows only, 25
- re-enable triggering from NNMi, 33

diagnostics, 37
- configuring, 38
- server, 12
- using, 38

diagnostics server, 12
- embedded, 12
- installing, 20
- removing, 34
- system preparation, 12
- uninstalling, 34
- upgrading, 20

E

embedded diagnostics server, 12

existing HP Operations Orchestration Central server, 14, 25

exporting topology maps to Visio, 40

H

hardware, supported, 9

HP Operations Orchestration Central, 12, 14

I

installing
- diagnostic flows only, 25
- embedded diagnostics server, 20
- NNM iSPI NET, 19

K

keytool utility, 16, 18

L

licensing
- checking license type, 30
- installing permanent license, 30
- NNM iSPI NET, 30
- obtaining additional licenses, 31
- permanent license, 30
- temporary license, 30

log files
- nnm.0.0.log, 43, 46
- nnm-ispi-net-server-installer.log, 41
- trapanalytics.0.0.log, 39

M

Microsoft Visio files, 40

N

nnm.0.0.log file, 43, 46

nnmdiagnostics.ovpl command, 32

NNMi, preparation, 11

NNM iSPI NET
- components, 37
- configuration parameters, 22, 27
- configuring diagnostics, 38
- description, 7
- diagnostics, 37
- disable triggering of diagnostic flows, 32
- installing, 19
- licensing, 30
- removing, 33
- SNMP trap analytics, 39
- topology map Visio export, 40
- troubleshooting, 41, 43
- uninstalling, 33
- upgrading, 20
- using diagnostics, 38
- Visio map files, 40

nnm-ispi-net-server-installer.log file, 41

nnmtrapconfig.ovpl command, 39

nnmtrapdump.ovpl command, 40

P

prerequisites
- diagnostics server, 12
- hardware, 9
- NNMi, 11
- software, 9

R

removing NNM iSPI NET, 33

S

server
- embedded diagnostics, 12
- existing HP OO Central, 25

SNMP trap analytics, 39

software, supported, 9

SSL certificates, 44

supported
- devices, 9
- hardware, 9
- HP Operations Orchestration Central, 9
- MySQL, 9
- software, 9
- web browser, 9

T

temporary license, 30

trap analytics, 39

trapanalytics.0.0.log file, 39

troubleshooting
diagnostics server installation, 41
NNM iSPI NET server installation, 41
running diagnostic flows, 43
Visio export functionality, 46

U

uninstalling NNM iSPI NET, 33

upgrading
diagnostic flows only, 20
embedded diagnostics server, 20
NNM iSPI NET, 20

users, creating on diagnostics server, 29

V

Visio map files, 40

X

XML files, 40