

# HP Automated Network Management (ANM)

HP Network Node Manager i, iSPIs for Performance, NET iSPI, and  
HP Network Automation

for the Windows operating system

Solution Version: 9.0

---

## Configuration Guide

Document Release Date: August 2010

Software Release Date: April 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 2005 - 2010 Hewlett-Packard Development Company, L.P

## Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

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

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

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

## Acknowledgements

- This product includes software developed by Apache Software Foundation (<http://www.apache.org/licenses>).
- This product includes OpenLDAP code from OpenLDAP Foundation (<http://www.openldap.org/foundation/>).

- This product includes GNU code from Free Software Foundation, Inc. (<http://www.fsf.org/>).
- This product includes JiBX code from Dennis M. Sosnoski.
- This product includes the XPP3 XMLPull parser included in the distribution and used throughout JiBX, from Extreme! Lab, Indiana University.
- This product includes the Office Look and Feels License from Robert Futrell (<http://sourceforge.net/projects/officelnfs>).
- This product includes JEP - Java Exclickion Parser code from Netaphor Software, Inc. (<http://www.netaphor.com/home.asp>).

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

**<http://h20230.www2.hp.com/selfsolve/manuals>**

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

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

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

# Support

Visit the HP Software Support web site at:

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

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

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

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

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

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

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**



---

# Table of Contents

<b>Welcome to This Guide .....</b>	<b>9</b>
Document Goals.....	9
How This Guide Is Organized .....	10
Who Should Read This Guide .....	10
Additional Online Resources.....	11
<b>Chapter 1: Introduction to ANM .....</b>	<b>13</b>
ANM Overview .....	13
ANM Deployment Architecture Example .....	15
Hardware and Software Requirements .....	16
ANM Project Planning.....	26
NNMi – Overview .....	27
NA – Overview .....	27
iSPIs – Overview .....	28
<b>Chapter 2: NNMi and NA Integration Configuration.....</b>	<b>29</b>
Overview.....	29
Set Up NNMi for Integration with NA .....	30
<b>Chapter 3: ANM Solution Verification .....</b>	<b>37</b>
Overview.....	37
ANM Verification Scenarios .....	37
<b>Index.....</b>	<b>47</b>

## Table of Contents



---

# Welcome to This Guide

This guide provides information for setting up and configuring the HP Automated Network Management (ANM) solution.

## **This chapter includes:**

- Document Goals on page 9
- How This Guide Is Organized on page 10
- Who Should Read This Guide on page 10
- Additional Online Resources on page 11

## **Document Goals**

This document supplies its readers with an overview of the ANM solution—a composite of various HP products that give customers the ability to manage and monitor their network devices. The document also describes a procedure for configuring the integration between NNMi and NA products (both included in the solution) and how to verify that the solution and integrations are working—using common customer scenarios. This guide does not supply a procedure for how to configure the solution’s products. This can be found in the individual product manuals.

The solution environment architecture chosen for this document is only an example of a typical and common deployment.

## How This Guide Is Organized

This guide contains the following chapters:

### Chapter 1 Introduction to ANM

Provides an introduction to ANM integrations and briefly describes how the following products work with each other:

- ▶ HP Network Node Manager i (NNMi)
- ▶ HP Network Automation (NA)
- ▶ HP Network Node Manager iSPI Performance for Metrics (Metrics iSPI)
- ▶ HP Network Node Manager iSPI Performance for Traffic (Traffic iSPI)
- ▶ HP Network Node Manager iSPI Performance for Quality Assurance (QA iSPI)
- ▶ HP Network Node Manager iSPI Network Engineering Toolset (NET iSPI)

### Chapter 2 NNMi and NA Integration Configuration

Describes the necessary steps to configure and verify the integration between NNMi and NA.

### Chapter 3 ANM Solution Verification

Provides verification scenarios depicting the necessary steps to verify the ANM Solution is working correctly.

## Who Should Read This Guide

This guide is intended for a system implementer or system administrator who will be implementing the ANM solution. This guide assumes that you have administrative access to all systems. The procedures in this guide may duplicate information available in the relevant documentation for these products, but is provided here for convenience.

---

**Note:** If you have any feedback or comments about this document, please contact [solutionpackagingandscp@hp.com](mailto:solutionpackagingandscp@hp.com).

---

## Additional Online Resources

**Troubleshooting & Knowledge Base** accesses the Troubleshooting page on the HP Software Support Web site where you can search the Self-solve knowledge base. Choose **Help > Troubleshooting & Knowledge Base**. The URL for this Web site is <http://h20230.www2.hp.com/troubleshooting.jsp>.

**HP Software Support** accesses the HP Software Support Web site. This site enables you to browse the Self-solve knowledge base. You can also post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. Choose **Help > HP Software Support**. The URL for this Web site is [www.hp.com/go/hpsoftwaresupport](http://www.hp.com/go/hpsoftwaresupport).

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)

To register for an HP Passport user ID, go to:

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

**HP Software Web site** accesses the HP Software Web site. This site provides you with the most up-to-date information on HP Software products. This includes new software releases, seminars and trade shows, customer support, and more. Choose **Help > HP Software Web site**. The URL for this Web site is [www.hp.com/go/software](http://www.hp.com/go/software).

Welcome to This Guide

# 1

---

## Introduction to ANM

This chapter includes:

### Concepts

- ANM Overview on page 13
- ANM Deployment Architecture Example on page 15
- Hardware and Software Requirements on page 16
- ANM Project Planning on page 26
- NNMi – Overview on page 27
- NA – Overview on page 27
- iSPi – Overview on page 28

## Concepts

### ANM Overview

ANM is a solution that integrates network fault detection, performance monitoring, configuration management and compliance, as well as incorporating the diagnostic and automation tools. It enables the ITILv3 best practices in the network domain—namely event, incident and problem management; change configuration; and release and deploy management. ANM enables the IT organization to:

- reduce the Mean Time to Repair (MTTR),
- increase the Mean Time Between Failure (MTBF),

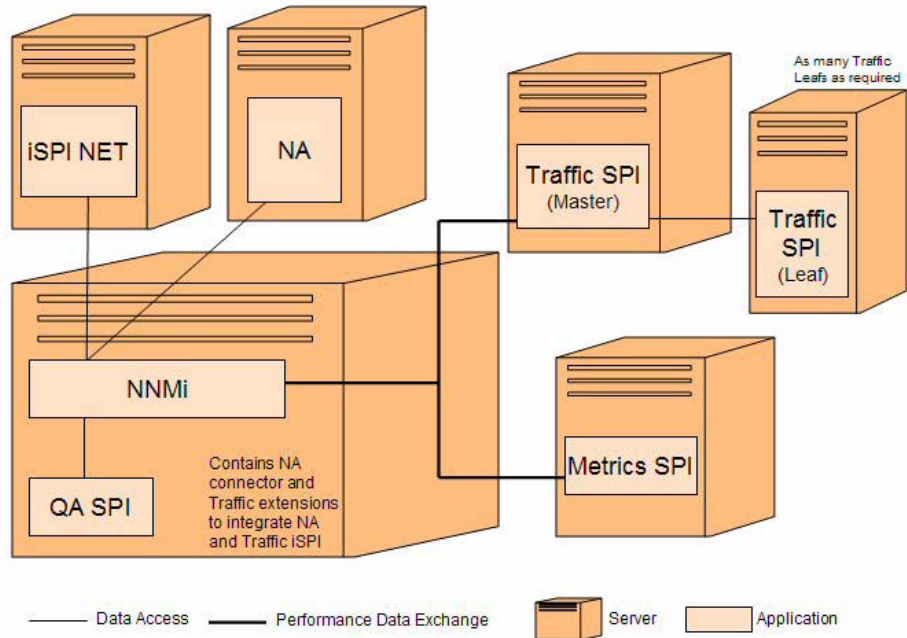
- become policy compliant,
- reduce Mean Time to Change network configuration,
- and increase the SLA with faster ROI.

The ANM solution is comprised of six individual, but integrated products that are brought together from the HP Network Management Center. The products that comprise the ANM 9.0 solution are:

- HP Network Node Manager i 9.0
- HP Network Automation 7.6
- HP Network Node Manager iSPI Performance for Metrics 9.0
- HP Network Node Manager iSPI Performance for Traffic 9.0
- HP Network Node Manager iSPI Performance for Quality Assurance 9.0
- HP Network Node Manager iSPI Network Engineering Toolset 9.0

## ANM Deployment Architecture Example

The following diagram displays a typical deployment of the ANM solution.




---

**Note:** The solution products offer a wide range of supported platforms and deployment compositions, including support for other operating systems, such as Linux, and also HA deployments. The deployment architecture described in this document is only one example. For more information, please refer to the support matrix documents at: <http://support.openview.hp.com/selfsolve/manuals>.

---

## Hardware and Software Requirements

The instructions in this document assume that products are installed in the default location. If this is not the case, be sure to use the path that was used in your deployment for all procedures mentioned in this document and referenced documents.

- ▶ NNMi – C:\Program Files (x86)\HP\HP BTO Software
- ▶ NA – C:\NA

---

**Important:** The QA iSPI, Net iSPI, Traffic iSPI, and Metrics iSPI are all important parts of the solution. Despite that, you can choose to not install some of them as long as you understand the capability reduction of the solution as a result of that.

If you choose to not install some of the iSPIs, be aware of the following:

- ▶ Traffic iSPI cannot be installed without Metrics iSPI.
- ▶ Scenario #1 in Chapter 3 is not relevant without Metrics iSPI installed.

During the iSPI installations, be sure to have your NNMi server details available as you will be asked to provide them. Be aware they are case-sensitive.

For installation instructions, see "Supported Versions" on page 17.

---

This section also includes:

- ▶ "Supported Versions" on page 17
- ▶ "Enterprise Hardware and Software Requirements" on page 18



## Supported Versions

Product	Version	instructions
NNMi	9.0 or later <b>Recommended:</b> 9.0	For installation instructions, see <i>HP Network Node Manager i Software Installation Guide</i> .
NA	7.60.02 or later <b>Recommended:</b> 7.60.02	For installation instructions, see <i>HP Network Automation Upgrade and Installation Guide</i> .
QA iSPI	9.0 or later <b>Recommended:</b> 9.0	For installation instructions, see <i>HP Network Node Manager i Software Smart Plug-in Performance for Quality Assurance Installation Guide</i> .
NET iSPI	9.0 or later <b>Recommended:</b> 9.0	For installation instructions, see <i>HP NNM iSPI Network Engineering Toolset Software Planning and Installation Guide</i> .
Traffic iSPI	9.0 or later <b>Recommended:</b> 9.0	For installation instructions, see <i>HP Network Node Manager iSPI Performance for Traffic Software Installation Guide</i> .
Metrics iSPI	9.0 or later <b>Recommended:</b> 9.0	For installation instructions, see <i>HP Network Node Manager i Software Smart Plug-in Performance for Metrics/Network Performance Server Installation Guide</i> .

---

**Important:** Make sure that each application you install is up and running before you perform any configuration steps.

---

## Enterprise Hardware and Software Requirements

These requirements are based on the following assumptions:

- ▶ Network environment size is between 3,000-8,000 devices.
- ▶ Only the embedded databases of the products are used in this architecture.
- ▶ All servers are Microsoft Windows Servers.
- ▶ The architecture of servers is as displayed in "ANM Deployment Architecture Example" on page 15.

---

**Note:** Anti-virus and backup software can interfere with the products' operation if the software locks files while the they are running. Any application that locks files should be configured to exclude the installation and data directories (selected in the installation directory).

Windows 2008 includes the concept of User Access Control (UAC). Users who are part of the Administrator group may not have full Administrator privileges. All scripts and commands associated with the products will detect and warn if the user is not enabled. Scripts and commands must be run with full Administrator access. To achieve full Administrator access, right-click the **Command Tool** icon and choose **Run as Administrator**.

Verify that all servers are on the same network segment without any firewalls between them. Having a firewall between the solution servers affects product performance.

---

## NNMi and QA iSPI Server Requirements

Recommendations	
<b>Hardware</b>	<ul style="list-style-type: none"> <li>▶ Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 4 CPU Cores</li> <li>▶ 16GB RAM</li> <li>▶ Virtual Memory (recommended to be double the RAM size)</li> <li>▶ 200GB free space (recommended that free space be on a different drive than the operating system). This also includes space for iSPI's shared data.</li> </ul>
<b>Operating System</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>▶ Windows Server 2003 x64 with Service Pack 2</li> <li>▶ Windows Server 2003 x64 R2 with Service Pack 2</li> <li>▶ Windows Server 2008 x64 Datacenter Edition with Service Pack 2</li> <li>▶ Windows Server 2008 R2 x64 Datacenter Edition</li> <li>▶ Windows Server 2008 x64 Enterprise Edition with Service Pack 2</li> <li>▶ Windows Server 2008 R2 x64 Enterprise Edition</li> </ul>
<b>Database</b>	<p>Embedded database on the NNMi management server:</p> <ul style="list-style-type: none"> <li>▶ NNMi automatically installs, initializes, and maintains the embedded database.</li> <li>▶ NNMi provides tools for re-initialization, backing up while online, and restoring the embedded database.</li> <li>▶ The embedded database performs well for most deployments.</li> </ul>

<b>Other Requirements</b>	<p>General Web Browser Requirements</p> <ul style="list-style-type: none"><li>▶ Disable all pop-up window blockers for the browser (see instructions on the NNMi console sign-in page or in the <i>HP Network Node Manager i Software Installation Guide</i>).</li><li>▶ Enable cookies for the browser (see instructions on the NNMi console sign-in page or in the <i>HP Network Node Manager i Software Installation Guide</i>).</li><li>▶ The resolution of the client display should be at least 1024x768.</li></ul> <p><b>Caution:</b> The following browsers are not supported:</p> <ul style="list-style-type: none"><li>▶ Microsoft Internet Explorer version 6 (browser causes layout problems)</li><li>▶ Apple Safari (all versions)</li><li>▶ Opera (all versions)</li><li>▶ Google Chrome (all versions)</li></ul> <p>Supported Web Browsers (also for remote clients)</p> <ul style="list-style-type: none"><li>▶ Microsoft Internet Explorer version 8.</li><li>▶ Microsoft Internet Explorer version 7.0.5730.11 or higher, with October 2007 or later Cumulative Patch for Internet Explorer 7. This patch increases the number of Internet Explorer cookies from 20 to 50, which is useful for saving more NNMi console table configurations.</li><li>▶ Mozilla Firefox version 3.6 or a newer minor version on a Windows or Linux client. The Firefox browser is available from <b><a href="http://www.mozilla.org/firefox">www.mozilla.org/firefox</a></b>. The Firefox browser works best if new windows are opened as separate windows, not tabs. For more information, see <i>Mozilla Firefox Known Problems</i> in the Release Notes.</li></ul>
---------------------------	---

For advanced sizing and platform support information, see

- ▶ [\*HP Network Node Manager i Software System and Device Support Matrix\*](#)
- ▶ [\*HP Network Node Manager i Software Smart Plug-in Performance for Quality Assurance System and Device Support Matrix\*](#)

---

**Note:** Links require HP Passport sign-in.

---

## NA Server Requirements

Recommendations	
<b>Hardware</b>	<ul style="list-style-type: none"> <li>▶ Intel Xeon or equivalent, 3.0+ GHz x 4 CPU Cores</li> <li>▶ 8GB RAM</li> <li>▶ Virtual Memory (recommended to be double the RAM size)</li> <li>▶ 100GB free space (recommended that free space be on a different drive than the operating system)</li> </ul>
<b>Operating System</b>	One of the following: <ul style="list-style-type: none"> <li>▶ Windows Server 2003 with Service Pack 2</li> <li>▶ Windows Server 2003 R2 with Service Pack 2</li> </ul>
<b>Database</b>	<ul style="list-style-type: none"> <li>▶ MySQL 5.0.58. (included in the installation kit) or Microsoft SQL Server 2005</li> <li>▶ Standard and Enterprise Edition SP2 on a remote server</li> </ul>
<b>Other Requirements</b>	<ul style="list-style-type: none"> <li>▶ Adobe® Flash Player 9.x and above (also on remote client)</li> <li>▶ Adobe® Acrobat Reader™ version 4.0 or higher, if you are viewing NA documentation from the NA server</li> <li>▶ NA supports the following browsers:               <ul style="list-style-type: none"> <li>▶ Mozilla Firefox 2.0.0.19, 2.0.0.20, and 3.x</li> <li>▶ Internet Explorer 6.x, 7.x</li> </ul> </li> <li>▶ Microsoft Excel 2000 or higher, if you are viewing summary reports from the NA server (also on remote client)</li> <li>▶ ActivePerl 5.8.x (for Windows)</li> <li>▶ Perl Net::SSH::Expect module (for using the Connect module with SSH)</li> </ul>

For advanced sizing and platform support information, see

▶ [\*HP Network Automation Upgrade and Installation Guide\*](#)

---

**Note:** Links require HP Passport sign-in.

---

## NET iSPI Server Requirements

Recommendations	
<b>Hardware</b>	<ul style="list-style-type: none"> <li>▶ Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 2 CPU Cores</li> <li>▶ 4GB RAM</li> <li>▶ 10GB free space (recommended that free space be on a different drive than the operating system)</li> </ul>
<b>Operating System</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>▶ Windows Server 2003 x64 with Service Pack 2</li> <li>▶ Windows Server 2003 x64 R2 with Service Pack 2</li> </ul> <p><b>Note:</b> Windows operating systems on Itanium Processor Family (IPF) are not supported.</p>
<b>Database</b>	MySQL versions 5.0.51b and later (included in the installation kit)
<b>Other Requirements</b>	For Web browser requirements, see "NNMi and QA iSPI Server Requirements" on page 19.

For advanced sizing and platform support information, see

- ▶ [HP Network Node Manager iSPI Network Engineering Toolset Diagnostics Server System and Device Support Matrix](#)

---

**Note:** Links require HP Passport sign-in.

---

## Traffic iSPI Server Requirements (Master Collector)

Recommendations	
<b>Hardware</b>	<ul style="list-style-type: none"> <li>▶ Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 4 CPU Cores</li> <li>▶ 8GB RAM</li> <li>▶ Virtual Memory (recommended to be double the RAM size)</li> <li>▶ 10GB free space (recommended that free space be on a different drive than the operating system)</li> </ul>
<b>Operating System</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>▶ Windows Server 2003 x64 with Service Pack 2</li> <li>▶ Windows Server 2003 x64 R2 with Service Pack 2</li> <li>▶ Windows Server 2008 x64 Datacenter Edition with Service Pack 2</li> <li>▶ Windows Server 2008 R2 x64 Datacenter Edition</li> <li>▶ Windows Server 2008 x64 Enterprise Edition with Service Pack 2</li> <li>▶ Windows Server 2008 R2 x64 Enterprise Edition</li> </ul> <p><b>Note:</b> Windows operating systems on Itanium Processor Family (IPF) are not supported.</p>
<b>Database</b>	Not applicable
<b>Other Requirements</b>	For Web browser requirements, see "NNMi and QA iSPI Server Requirements" on page 19.

For advanced sizing and platform support information, see

- ▶ [HP Network Node Manager i Software Smart Plug-in Performance for Traffic System and Device Support Matrix](#)

---

**Note:** Links require HP Passport sign-in.

---

## Traffic iSPI Server Requirements (Leaf Collector)

Recommendations	
<b>Hardware</b>	<ul style="list-style-type: none"> <li>▶ Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 4 CPU Cores</li> <li>▶ 6GB RAM</li> <li>▶ Virtual Memory (recommended to be double the RAM size)</li> <li>▶ 10GB free space (recommended that free space be on a different drive than the operating system)</li> </ul>
<b>Operating System</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>▶ Windows Server 2003 x64 with Service Pack 2</li> <li>▶ Windows Server 2003 x64 R2 with Service Pack 2</li> <li>▶ Windows Server 2008 x64 Datacenter Edition with Service Pack 2</li> <li>▶ Windows Server 2008 R2 x64 Datacenter Edition</li> <li>▶ Windows Server 2008 x64 Enterprise Edition with Service Pack 2</li> <li>▶ Windows Server 2008 R2 x64 Enterprise Edition</li> </ul> <p><b>Note:</b> Windows operating systems on Itanium Processor Family (IPF) are not supported.</p>
<b>Database</b>	Not applicable
<b>Other Requirements</b>	For Web browser requirements, see "NNMi and QA iSPI Server Requirements" on page 19.

For advanced sizing and platform support information, see

- ▶ [\*HP Network Node Manager i Software Smart Plug-in Performance for Traffic System and Device Support Matrix\*](#)

---

**Note:** Links require HP Passport sign-in.

---



## Metrics iSPI Server Requirements

Recommendations	
<b>Hardware</b>	<ul style="list-style-type: none"> <li>▶ Intel 64-bit (x86-64) or AMD 64-bit (AMD64) x 8 CPU Cores</li> <li>▶ 12-24GB RAM</li> <li>▶ Virtual Memory (recommended to be double the RAM size)</li> <li>▶ 800GB free space (recommended that free space be on a different drive than the operating system). This also includes space for Traffic iSPI data.</li> </ul>
<b>Operating System</b>	<p>One of the following:</p> <ul style="list-style-type: none"> <li>▶ Windows Server 2003 x64 with Service Pack 2</li> <li>▶ Windows Server 2003 x64 R2 with Service Pack 2</li> <li>▶ Windows Server 2008 x64 Datacenter Edition with Service Pack 2</li> <li>▶ Windows Server 2008 R2 x64 Datacenter Edition</li> <li>▶ Windows Server 2008 x64 Enterprise Edition with Service Pack 2</li> <li>▶ Windows Server 2008 R2 x64 Enterprise Edition</li> </ul> <p><b>Note:</b> Windows operating systems on Itanium Processor Family (IPF) are not supported.</p>
<b>Database</b>	Not applicable
<b>Other Requirements</b>	For Web browser requirements, see "NNMi and QA iSPI Server Requirements" on page 19.

For advanced sizing and platform support information, see

- ▶ [HP Network Node Manager i Software Smart Plug-in Performance for Metrics/Network Performance Server System and Device Support Matrix](#)

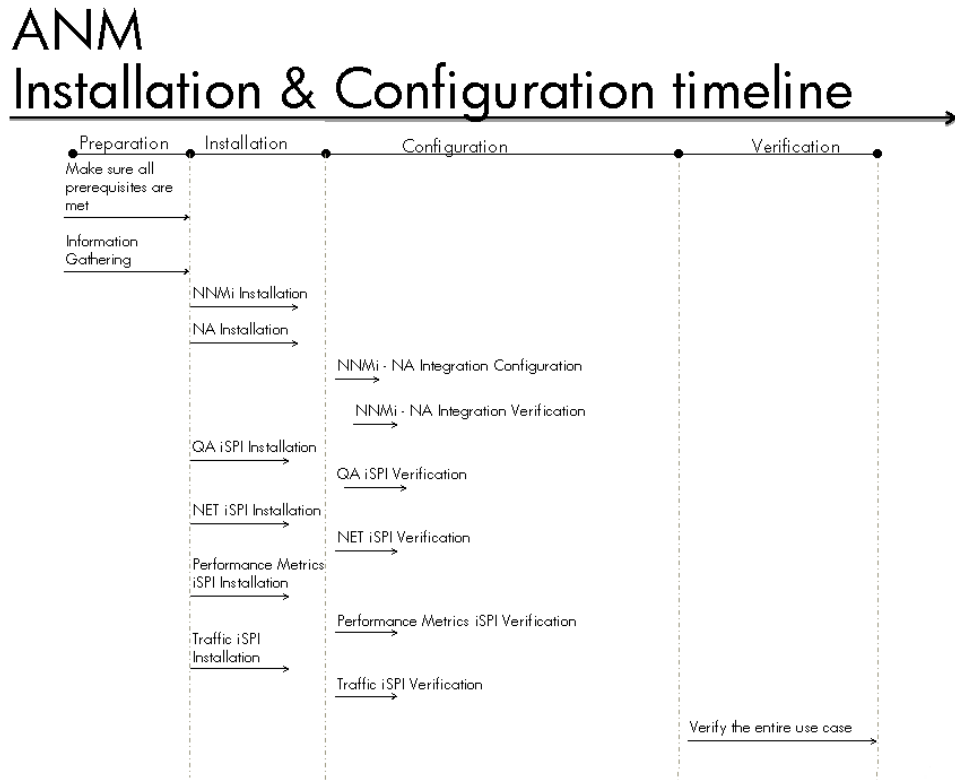
---

**Note:** Links require HP Passport sign-in.

---

## ANM Project Planning

The following diagram provides a visual display of the various tasks that must be done in order to use the ANM solution.



---

**Note:** Information gathering must include:

- ▶ Vendor of devices monitored in the organization
  - ▶ Network architecture and any security requirements needed to be addressed
  - ▶ IP range for initial discovery
  - ▶ SNMP version and community strings
  - ▶ User name and password for accessing devices from NA
- 

## **NNMi – Overview**

HP Network Node Manager i Software contains a toolset to help you maintain a healthy network across your organization. NNMi can discover network nodes (such as switches and routers) on an ongoing basis, providing an up-to-date representation of the network topology. As NNMi maintains an accurate picture of the network, it also helps you handle problems through management by exception—the ability to pinpoint network problems by using event correlation and root cause analysis (RCA). Unlike other network management software, NNMi applies sophisticated RCA algorithms to an accurate, ever-changing view of network topology to support dynamic fault management.

## **NA – Overview**

HP Network Automation provides an enterprise class solution that tracks and regulates configuration and software changes across routers, switches, firewalls, load balancers, and wireless access points. NA provides visibility into network changes, enabling an IT staff to identify and correct trends that could lead to problems, while mitigating compliance issues, security hazards, and disaster recovery risks. NA also captures full audit trail information about each device change.

## **iSPIs – Overview**

The Smart Plug-ins (SPIs) provide valuable insight into the current health and ongoing trends in your network, allowing you to increase availability and performance, while lowering associated support costs and improving capacity management and planning.

**NNM iSPI Performance for QA (QA iSPI)** extends the capability of NNMi to monitor the quality of traffic flows in the network. QA iSPI will help the network engineers to identify and measure RTT, packet loss, and jitter in the network, by collecting data from preconfigured probes or IP SAL tests, to proactively ensure the network service level which they provide to their customers.

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

**HP Network Node Manager iSPI Performance for Traffic Software (Traffic iSPI)** extends the capability of NNMi to monitor the performance of the network. The NNM iSPI for Traffic facilitates enrichment of the obtained data from the IP flow records that are exported by the routers and allows you to diagnose IP traffic problems throughout your network.

**HP Network Node Manager i Software Smart Plug-in Performance for Metrics (Metrics iSPI)** provides the core performance management capability to NNMi by gathering and monitoring the metric data polled by NNMi from different network elements.

# 2

---

## NNMi and NA Integration Configuration

This chapter includes:

### Concepts

- ▶ Overview on page 29

### Tasks

- ▶ Set Up NNMi for Integration with NA on page 30

## Concepts

### Overview

The HP NNMi–HP NA integration adds menu items to the NNMi console for opening connections to NA and for viewing configuration information on devices managed by NA. These menu items and other features in the integration provide the following functionality:

- ▶ View detailed device information, including vendor, model, modules, operating system version, and recent diagnostic results
- ▶ View device configuration changes and configuration history
- ▶ Compare configurations (typically the most recent and last previous configurations) to see what changed, why, and who made the changes
- ▶ View device compliance information
- ▶ Run NA diagnostics and command scripts from NNMi nodes
- ▶ Incident forwarding such that NA forwards notifications to NNMi about changes to device configuration and so on

- ▶ Suppress unnecessary incidents by setting NNMi nodes to out of service status while performing maintenance tasks on the device through NA
- ▶ (NNM iSPI NET) Detect connections with mismatched speed or duplex configurations

This section describes the necessary steps to configure and verify the integration between NNMi and NA.

## Tasks

### **Set Up NNMi for Integration with NA**

This task lists the steps necessary to configure NNMi in order to perform integration with NA.

This task includes the following steps:

- ▶ "Prerequisites" on page 30
- ▶ "Configure NNMi-NA Integration" on page 31
- ▶ "NNMi-NA Integration Verification" on page 35

#### **Prerequisites**

The NNMi and NA recommended versions are:

- ▶ NNMi Version 9.0
- ▶ NA Version 7.6 Patch 2 (7.60.02)

NNMi and NA can be installed on the same computer or on different computers.

Before you begin configuring the NNMi-NA integration, copy the following file to the NNMi server:

- ▶ If NNMi and NA are installed on the same server, from the NA kit, copy **na\_nnm\_coresidency\_windows.exe**.
- ▶ If NNMi and NA are installed on different servers, from the NA kit, copy **na\_nnm\_connector\_windows.exe**.

If NNMi and NA are installed on different servers, confirm that you can open the management console of NNMi from the NA server (**http://<NNMi Server Name>:<Port>/nnm**) and you can open the management console of NA from the NNMi server (**https://<NA Server Name>:<Port>**).

## Configure NNMi-NA Integration

**Before running the NNMi-NA connector installation:**

- 1** Log on to NNMi using your administrator user name or system user name.
- 2** Go to the **Configuration** workspace and click the **User interface** configuration. The User Interface configuration window opens.
- 3** On the **User Accounts** tab, click the **New** button. The Account Mapping window opens.
- 4** From the **Account** drop-down list, select **New**. The User Account window opens.
- 5** In the User Account window, fill in the details. Choose a user name that indicates this is a user for an NA integration.




---

**Note:** Remember this user name and password. You will need them in the following steps.

---

- 6** Click **Save and Close**.
- 7** In the Account Mapping window, verify that the user you have just created appears in the **Account** field.

- 8** In the **Role** field, select **Administrator**.
- 9** Click **Save and Close**.
- 10** In the User Interface configuration window, click **Save and Close**.

**To install and configure the HP NNM - HP NA integration:**

- 1** Log on to the NNMi server:
  - a** If NNMi and NA are installed on the same server, double-click **na\_nnm\_coresidency\_windows.exe**.
  - b** If NNMi and NA are installed on the different servers, double-click **na\_nnm\_connector\_windows.exe**.

The NA - HP NNM Connector dialog box opens.

- 2** In the Introduction dialog box, click **Next**.
- 3** In the Detect HP NNM dialog box, click **Next**.
- 4** In the Choose Install Folder dialog box, click **Next**.
- 5** In the NA Server Info dialog box, enter the following details and click **Next**.

Name	Recommended Value	Description
<b>Hostname</b>	<user defined>	Host name of your NA server For example: server.domain
<b>Username</b>	<user defined>	Administrative user configured in the NA installation
<b>Password</b>	<user defined>	Password of the administrator or system user
<b>Confirm password</b>	<user defined>	Password verification

- 6** In the Scheduled Device Import dialog box, click **Next**.



- 7** In the NNM Server Info dialog box, enter the following details and click **Next**.

Name	Recommended Value	Description
Hostname	<user defined>	Host name of your NA server For example: server.domain
Http Port	80	Default port for NNMi If you changed the default port (80), refer to <b>NNMi Help for Administrators</b> for information on how to retrieve it.
Username	<user defined>	User name specified before running the NNMi-NA connector installation as defined in Step 5 on page 31
Password	<user defined>	Password specified before running the NNMi-NA connector installation as defined in Step 5 on page 31
Confirm password	<user defined>	Password verification

- 8** In the Choose Shortcut window, click **Next**.
- 9** In the Pre-Installation dialog box, click **Install**.
- 10** In the Install Complete dialog box, click **Next**.
- 11** Open the browser and enter **http://<NNMi Server Name>:<Port>/nnm**. The NNMi log-on page opens.
- 12** Enter the user name and password of an administrator account.
- 13** Select **Integration Module Configuration > HP NA**. The HP NNMi-HP NA Integration Configuration window opens.
- a** Select the **Enable Integration** checkbox.
  - b** Confirm that the **HP NNMi SSL Enabled** checkbox is not selected and enter the NNMi server details you specified in Step 5.
  - c** Confirm that the **HP NA SSL Enabled** checkbox is not selected and enter the NA server details you specified in Step 7.

- d** In the **HP NA Connection Check Interval (hrs)** field, enter 1 hour and click **Submit**. The integration is enabled and a success message appears.
- 14** Log on to NA using your administrator account name or any other privileged NA user account name.
- 15** In the menu at the top of the Home page, select **Devices > Inventory**.
- 16** From the list of devices imported from NNMi, run the **Discover Driver** task.
- 17** In the **Select...** field at the top of the list, select **All devices**.
- 18** In the **Actions...** field, select **Discover Driver**.
- 19** In the **Task Parameters**, select the date and time you wish to run this task and click **Save Task**.

---

**Note:** It is recommended to set the date and time values to run this task as soon as possible.

---

The **Discover Driver** task ends successfully, and NA automatically starts the **Take Snapshot** task and **Diagnostics** task for each device. If the **Discover Driver** task fails, refer to the NA documentation for troubleshooting.

---

**Note:** To automate importing of devices from NNMi to NA, use the **Windows Scheduled Task** function to run the **C:\NA\nnmimport.bat** script every day.

For details on filtering devices from the import process, see the *NNMi Integration User's Guide* in your NA documentation.

---

## NNMi-NA Integration Verification

To verify the NNMi-NA integration:

- 1** Log on to NA using your administrator account name or other privileged NA user account name.
  - a** In the menu at the top of the Home page, select **Devices > Inventory**.
  - b** Confirm that all the devices listed in NNMi were imported to NA.
- 2** Log on to NNMi using your administrator account name or other privileged NNMi user account name.
  - a** Go to the **Configuration** workspace and click **Incident Configuration**.
  - b** In the **Incident Configuration** window, go to the **SNMP Traps** tab and search for definitions for traps **NASnmpTrapv1** and **NASnmpTrapv2**.

If it is not visible, run the following command through CLI:

```
nnmconfigimport.ovpl -u <AdminUser> -p <Password> -f  
"%NnmInstallDir%\App\bin\incidentconfig.xml"
```
  - c** Close the **Incident Configuration** window.
- 3** Log on to NA using your administrator user name or system user name.
- 4** In the upper menu, select **Administrative Settings > 3rd Party Integrations > NNM Connection Test**.

The success message "**NNM Integration Connection Test is successful.**" is displayed, verifying that NA can communicate with NNMi web services.

---

**Note:** If an error message is displayed, confirm that you configured the integration correctly or contact Customer Support.

---



# 3

---

## ANM Solution Verification

This chapter includes:

### Concepts

- ▶ Overview on page 37

### Tasks

- ▶ ANM Verification Scenarios on page 37

## Concepts

### Overview

This section provides verification scenarios depicting the necessary steps to verify the ANM Solution is working correctly.

## Tasks

### ANM Verification Scenarios

This chapter describes the following verification scenarios:

- ▶ "Scenario #1: High Error Rate" on page 38
- ▶ "Scenario #2: Preventing False Alarms on Devices Undergoing Maintenance" on page 43

## Scenario #1: High Error Rate

The iSPI for Performance Metrics is monitoring the error rate and utilization of interfaces across switches in the network.

In our scenario, the iSPI recognizes an interface with a high error rate and generates an incident. The operator then reports this to a Network Engineer who opens the NNMi to view the incident's details. In order to see additional details on this interface configuration, the Network Engineer opens the device configuration via NA to see which duplex is configured on this interface, and check if the device configuration had been recently changed.

A high error rate on an interface usually causes the workstation, server, or any other device connected to that interface to work significantly slower.

Expected outcomes:

- ▶ NNMi Performance for Metrics iSPI will recognize a problem and report it.
- ▶ Network Engineer will use NNMi and NA as tools to check the problem and repair it.

---

**Note:** This scenario will work in most organizations since this a common issue. You can also use a low threshold value of Interface Utilization to purposely generate a high Interface Utilization incident for testing.

---

The ANM Solution's products used in this scenario are:

- ▶ NNMi 9.0
- ▶ NA 7.6 Patch 2 (7.60.02)
- ▶ iSPI for Performance Metrics

### Scenario Prerequisites

- ▶ NNMi discovered most network devices, including the user's switches.
- ▶ All devices were imported into NA and their configuration was successfully drawn into NA.

## Configuration Steps

**1** Log on to NNMi using your administrator user name or system user name.

**2** In the **Configuration** workspace, select **Interface Groups**.



**3** Click the **New** button to create a new interface group with the following values:

Field	Value
Name	Ethernet interfaces
Notes	Interface group general notes
ifType Filters	ethernetCsmacd
NNM iSPI Performance>Add to filter list	Selected



**a** In the **ifType Filters** tab, click the **New** button to create a new filter.

**b** In the ifType Filters window, in the ifType field, enter ethernetCsmacd.

**c** Click **Save and Close**.

---

**Note:** For more information, click Help.

---

**4** In the Interface Groups window, click **Save and Close**.

**5** In the **Configuration** workspace, select **Monitoring Configuration**.



- 6** In the **Interface Settings** tab, click the **New** button to create a new setting with the following values:

Field	Value
Basics: Ordering	90
Basics: Interface Group	Ethernet interfaces
Performance Monitoring	Selected
Performance Monitoring	1 minute



- 7** In the **Threshold Settings** tab, click the **New** button to create two new threshold setting rates.

- a** For the **Input Error Rate**, enter the following values:

Field	Value
Monitored Attribute	Input Error Rate
High Value	2
High Rearm Value	1
High Trigger Count	1
Low Value	0
Low Rearm Value	0.01
Low Trigger Count	1



- b** After filling in the values, click the **Save and New** button.

- c** For the **Output Error Rate**, enter the following values:

Field	Value
Monitored Attribute	Output Error Rate
High Value	2
High Rearm Value	1
High Trigger Count	1



Field	Value
Low Value	0
Low Rearm Value	0.01
Low Trigger Count	1

- d** After filling in the values, click **Save and Close**.
- 8** In the new Interface Settings window, click **Save and Close**.
- 9** In the Monitoring Configuration window, click **Save and Close**.
- 10** In the **Configuration** workspace, select **Incidents Configuration**.
- 11** In the Incidents Configuration window, select the **Management Events** tab.
- 12** Look for incidents named **InterfaceOutputErrorRateHigh** and **InterfaceInputErrorRateHigh**. If the **Enabled** column value for those incidents is not selected, then open each one of them, check the **Enabled** check-box, and click **Save and Close**.
- 13** In the Incidents Configuration window, click **Save and Close**.
- 14** After completing the configuration, wait ~15-20 minutes. If no performance incident appears, perform the above configuration on Interface Utilization attributes.

### Procedure

- 1** Log on to NNMi using an operator user name
- 1** Go to the **Incident Management** workspace.
- 2** Select **Open Key Incidents**.
- 3** Confirm that the quick filtering selection boxes located at the toolbar at the top of the view are set to **Last Hour** and **Networking Infrastructure Devices**.
- 4** Between the events displayed, an incident is listed with a message such as: **High input error rate on interface <Interface Name>**.
- 5** Click the **Open** button next to the incident.

The Incident window opens and all details of this incident are displayed.

- 6 From the Incident window menu, select **Actions > View HP NA Device Configuration**.

The NA logon screen opens.

- 7 Log on to NA using your administrator account name or any other privileged NA user account name.

The device's current configuration is displayed.

- 8 Look for the interface related to the incident and check what the current duplex configuration is.

- 9 The Network Engineer can use one or more of the following processes:

- a To check if the device configuration has changed in the last few days: From the NA screen, in the menu bar at the top of the configuration, select **View > Configuration Changes**.

To fix the duplex configuration:

- From the NA screen, in the menu bar at the top of the configuration, select **Edit > Edit & Deploy Configuration** to edit and deploy the entire configuration.
- Alternatively, select **Provision > Run Command Script** in the New Task window. The Network Engineer can only run the commands necessary to change this interface duplex.
- b To check the interface performance history: From the Incident window opened in Step 5 above, click the selection button near the **Source Object** field value (which contains the interface name) and select **Open**.

In the top menu of the Interface window, select **Actions > Reporting-Report Menu**. The NNM iSPI Performance window opens listing all reports. The recommended report is Chart Detail. Under the name of the report, the letters **H D W M** are displayed. Select **D** to view the previous 24H history.

- 10 After the problem is fixed, the incident in NNMi closes automatically and the threshold monitor rearms.

## Scenario #2: Preventing False Alarms on Devices Undergoing Maintenance

In every organization, Network Engineers are constantly making changes to the network. Sometimes these changes involve shutting down network devices or making some of the services they supply unavailable. When that occurs, you do not want incidents to appear on those devices while you are working with them. NA <-> NNM integration allows you to avoid these false alarms and also gives the user the ability to determine when these devices will return to monitoring in NNMi, by manually modifying the node to be managed.

Expected outcomes:

- NNMi will not display device incidents while undergoing maintenance.
- Integration functionality allows the operator to return the device to monitoring as needed.

The ANM Solution's products used in this scenario are:

- NNMi 9.0
- NA 7.6 Patch 2 (7.60.02)

### Scenario Prerequisites

- NNMi discovered most network devices, including the user's switches.
- All devices were imported to NA and their configuration was successfully drawn into NA.


### Configuration Steps

- 1 Log on to NA using your administrator user name or system user name.
- 2 In the upper menu, select **Administrative Settings > 3rd Party Integrations > NNM Connection Test**.

The success message "**NNM Integration Connection Test is successful.**" is displayed, verifying that NA can communicate with NNMi web services.

**Note:** If an error message is displayed, go back to "NNMi and NA Integration Configuration" on page 29 and confirm that you configured the integration correctly or contact Customer Support.

---

- 3** Return to the Admin menu and select **Administrative Settings > 3rd Party Integrations**.
- 4** In the **Out-of-Service Events** text box, press and hold the **CTRL** key on your keyboard and select the **Take Snapshot** task.
-  **5** Click **Save**.

### **Procedure: Phase 1—Simulating Network Maintenance on a Device**

- 1** Log on to NA using your administrator account name or any other privileged user account name.
- 2** In the upper menu, select **Devices > Inventory**.
- 3** Select one of the devices.
- 4** In the **Actions** drop-down menu, at the top of the list, select **Take Snapshot**.

---

**Note:** Confirm that this device has a definition for access details as part of a Device Password Rule or specific device credentials. See HP Network Automation User Guide for further details.

---

- 5** In the New Task screen, confirm that **Start as soon as possible** is selected and that the correct device is listed in the **Applies to** field.
- 6** Click the **Save Task** button. Watch the Task status. If it finishes successfully, go to the next step.

If it does not finish successfully, try debugging the problem by selecting the **Run Again** option in the upper-right area of the window. You will return to the New Task screen. Confirm that **Store Complete session log** is selected and click the **Save Task** button. The results of this task allow you to further understand what the source of the problem is.

### **Procedure: Phase 2—Verifying Node Status After Maintenance**

- 1** Log on to NNMi using an Operator user account.
- 2** Go to **Management Mode** workspace and select **Unmanaged Nodes**.
- 3** In the list displayed on the right side, find the node to run the **Take Snapshot** task.



- 4** Click the **Open** button.

The Node Details window opens.

- 5** Confirm the **Node Management Mode** field value is set to **Out of Service**. This confirms that this part of the integration is working.

---

**Note:** If the Node Management Mode field value is not set to Out of Service, troubleshoot using the NNMi-NA manuals or contact Customer Support.

---

### Procedure: Phase 3—Rolling Back Configuration

The Operator must confirm the node is OK before returning it to managed service.

- 1** Go to the Actions menu and select **Management Mode > Manage**. NNMi will automatically poll the device for its status when it is returned to be managed. This must be confirmed.
- 2** To confirm the result of the status poll, you can:
  - a** Return to the Actions menu and select **Status Poll**. Watch the results of the test and confirm everything is UP.
  - b** Close the Status Poll window, click the **Save** button on the Node Details window, then click **Refresh** and watch the Status field.
- 3** Close the Node Details window.



---

# Index

## A

- ANM
  - architecture 15
  - overview 13
  - supported product versions 17

## H

- hardware requirements 16, 18
- HP Software Support Web site 11
- HP Software Web site 11

## I

- installation requirements 30
  - NA 21
  - NET iSPI 22
  - NNMi 19
  - Performance Metrics 25
  - Traffic iSPI 23, 24
- integration overview
  - NNMi and NA Integration Configuration 29, 37
- iSPI
  - overview 28

## K

- Knowledge Base 11

## N

- NA
  - overview 27
- NET iSPI
  - installation requirements 22
- NNMi
  - overview 27
- NNMI-NA integration
  - overview 29, 37

## O

- online resources 11
- overview
  - NNMi and NA Integration Configuration 29, 37

## P

- Performance Metrics
  - installation requirements 25

## R

- requirements
  - hardware and software 16, 18

## S

- software requirements 16, 18
- supported versions 17

## T

- Traffic iSPI
  - installation requirements 23, 24
- Troubleshooting and Knowledge Base 11

