HP Network Automation Software

For the Windows®, Linux, and Solaris operating systems

Software Version: 9.22.01

Administration Guide

Document Release Date: October 2015
Software Release Date: November 2014

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

Intel and Intel Itanium are trademarks of Intel Corporation in the U.S. and other countries.

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

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

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

For the full Oracle license text, after product installation see the `<NA_HOME>/server/license` directory on the NA core server.

Acknowledgements

This product includes software developed by the Apache Software Foundation. (http://www.apache.org)

Parts of this software Copyright © 2003-2008 Enterprise Distributed Technologies Ltd. All Rights Reserved. (http://www.enterprisedt.com)

Documentation Updates

This guide's title page 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

You can visit the HP Software Support Online web site at:

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

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

HP Software Support Online 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 HP Software 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 find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

Contents

1 About This Guide

This guide contains a collection of information and best practices for administering HP Network Automation Software (NA). This guide is for an expert system administrator, network engineer, or HP support engineer with experience deploying and managing networks in large installations.

This guide assumes that you have already installed NA and that you are familiar with start-up configuration tasks. To learn more about these tasks, see the *NA Installation and Upgrade Guide* and the NA help.

HP updates this guide between product releases as new information becomes available. For information about retrieving an updated version of this document, see Documentation Updates on page 3.

Revision History

Table 1 lists the major changes for each new release of this document.

Table 1 Document Changes

Document Release Date	Description of Major Changes
May 2012 (9.20)	First publication for NA version 9.20.
September 2012 (9.20 Patch 1)	Added the following chapters: • Ports • Tuning NA Performance • Localization Concerns • Troubleshooting an Abnormal Condition on the NA Server • Configuring the NA Determination of Which User Changed a Device
December 2012 (9.21)	Minor updates to the following chapters: • Ports (added the SSH and telnet ports for the Windows operating system) • Changing NA Credentials When Connecting to a New Database Location (revised the instructions for using exiting tc_tools to correspond to the updated tool)

Table 1 Document Changes

Document Release Date	Description of Major Changes
May 2013 (9.22)	Added the following chapters: • Configuring NA to Support PKI User Authentication • Configuring the Diagnostic Policy Compliance Check Setting Default • Running NA with Minimal Database User Privileges Significant updates to the following chapters: • Using Certificates with NA (new section: Adding a CA Root Certificate to NA) • Configuring the Task Completion Email Content (new and revised content)
April 2014	Changes to the Using Certificates with NA chapter: revised the Adding a CA-Signed Certificate to NA topic to include importing the `CA.crt` file into the Truecontrol trust store.
November 2014 (9.22.01)	Updated the following chapters: • Enabling FIPS Mode • Full-Text Search of Configuration Text (Oracle and SQL Server) (new section: Adding a Reminder to Use Full-Text Search Where Applicable) Added the following chapters: • Starting an External Application as a Non-Root User (Linux and Solaris only) • Configuring NA to Permit Editing of Tasks Waiting for Approval • Setting the Update Device Software Task Status to Reflect Child Task Status • Configuring NA to Warn Before a Task Modifies a Device • Configuring NA to Sort Device Groups at the Top of the Applies To List • Setting the Preferred Credentials for Accessing a Device • Configuring NA to Run Windows PowerShell Scripts • Customizing the Banner on the NA SSH Server

2 HP Network Automation Software Architecture

The NA architecture diagram in Figure 1 illustrates the NA Core components and their logical connections. The diagram also includes external products and components with which NA integrates.

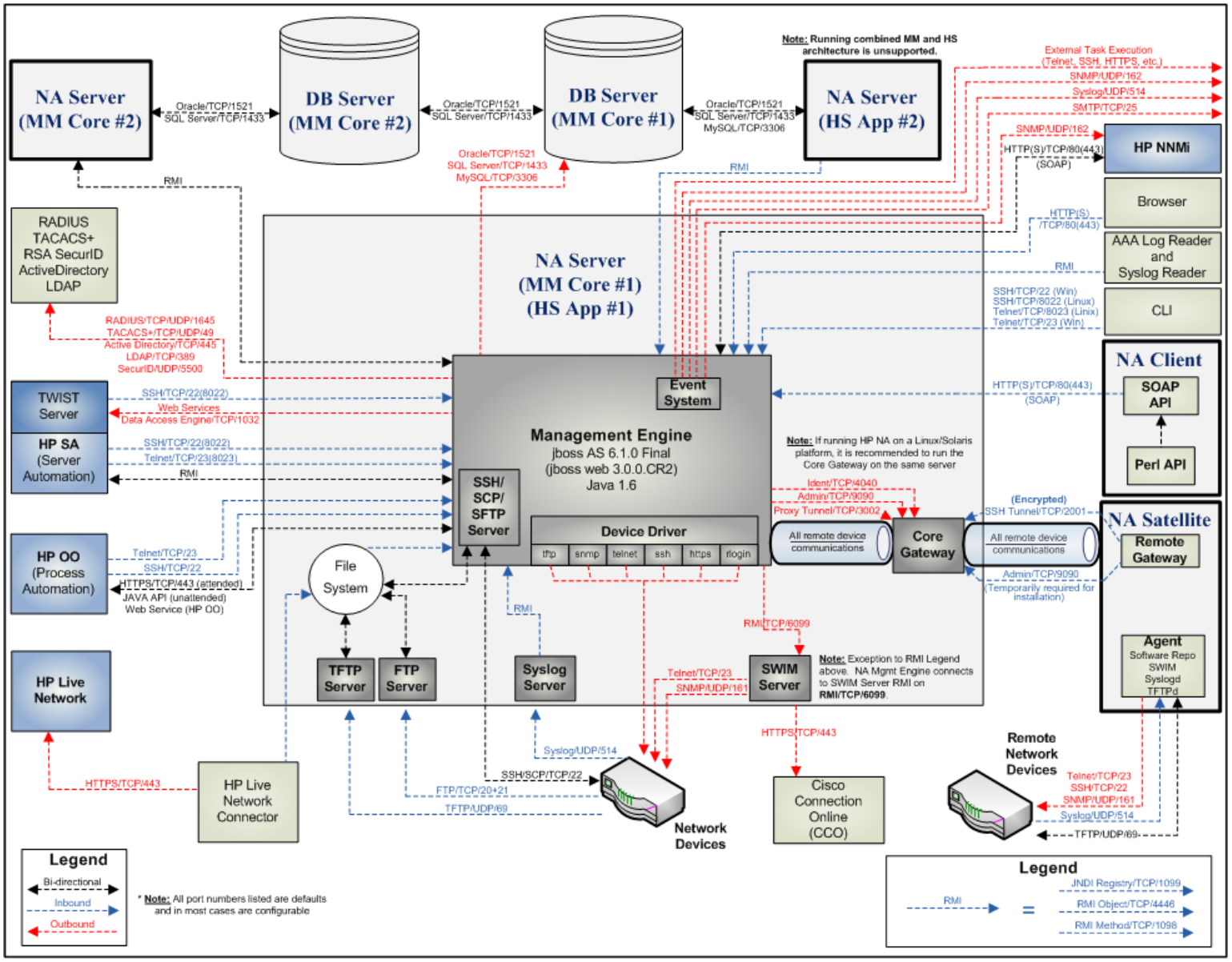
An NA Core is comprised of both an NA server and a database server. The center of the diagram shows the NA server, identified as both the Multimaster Core (MM) #1 and Horizontal Scalability (HS) App #1. Just above the NA server is the database server that is part of Multimaster (MM) Core #1 or the Horizontal Scalability configuration.

NA Cores can be meshed together to provide data replication, high availability, and disaster recovery. In the upper left of the diagram are a second NA server and a second database server, both identified as MM Core #2, along with the required connections between the database servers of MM Core #1 and MM Core #2 to create the mesh.

Included in the NA server are the NA Management Engine, the Core Gateway, the TFTP server, the FTP server, the Syslog server, and the SWIM server processes. The SSH/SCP/SFTP server and the Event System shown inside the NA Management Engine are embedded within the NA Management Engine process.

Around the perimeter of the diagram are the external entities with which the NA Core server integrates. Each connection from the NA Management Engine to an external entitiy identifies the service name, protocol, port number, and direction (bidirectional, inbound, or outbound) with respect to the NA Management Engine.

Figure 1 NA Architecture



3 Ports

This chapter shows ports that Network Management Center (NMC) products use in network communications.

The ports listed in NMC Well-Known Ports on page 14 are those used by all NMC products, sorted by port number to help you identify any possible port conflicts.

In addition, subsequent sections document the ports used by the individual products that comprise NMC. See the respective sections that follow:

NMC Well-Known Ports

Table 2 shows the ports that Network Management Center (NMC) products use in network communications. The ports listed in Table 2 are those used by all NMC products, sorted by port number to help you identify any possible port conflicts. If port conflicts occur between products, you can change most of these port numbers as shown in the *Change Configuration* column.

Table 2 Ports Used by NMC Products

Port	NMC Product	Type	Name	Purpose	Change Configuration
22	NA Core	TCP	`SSH Server Port`	SSH port from the NA client to the NA server on the Windows operating system	See "Telnet/SSH Page Fields" in the NA help.
23	NA Core	TCP	`Telnet Server Port`	Telnet port from the NA client to the NA server on the Windows operating system	See "Telnet/SSH Page Fields" in the NA help.
69	NA Core	UDP	`TFTP Port`	Network devices to the NA server	Change not supported
80	NA Core	TCP	`HTTP Port`	HTTP port from the NA client to the NA server	Contact your Support representative for assistance.
80	NNMi	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI & Web Services - In GNM configurations NNMi uses this port to establish communication from the global manager to the regional manager - Once this port is open, it becomes bi-directional	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX). You can also change this during installation.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
162	NNMi	UDP	`trapPort`	SNMP trap port	Modify using the `nnmtrapconfig.ovpl` Perl script. See the *nnmtrapconfig.ovpl* reference page, or the UNIX manpage, for more information.
443	NA Core	TCP	`HTTPS Port`	HTTPS port from the NA client to the NA server	Contact your Support representative for assistance.
443	NNMi	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI & Web Services	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
514	NA Core	UDP	`Syslog Port`	Receive syslog messages from network devices on the NA server	See "Configuring the NA Syslog Server" in the NA Installation and Upgrade Guide.
1098	NA Core	TCP	`RMI Activation Port`	Port between NA clients and the NA Management Engine and between the NA Management Engines in separate NA Cores. NA clients can include: -NA Syslog Server -NA Connectors -AAA Log Reader -Syslog Reader -Customer-written API scripts (For information, see the NA API User Guide and the NA CLI/API Command Reference.)	Contact your Support representative for assistance.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
1098	NNMi	TCP	`nmsas.server.port.naming.rmi`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
1099	NA Core	TCP	`RMI Registration Port`	Port between NA clients and the NA Management Engine and between the NA Management Engines in separate NA Cores. NA clients can include: -NA Syslog Server -NA Connectors -AAA Log Reader -Syslog Reader -Customer-written API scripts (For information, see the NA API User Guide and the NA CLI/API Command Reference.)	Contact your Support representative for assistance.
1099	NNMi	TCP	`nmsas.server.port.naming.port`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
1433	NA Core	TCP	`Microsoft SQL Server Port`	Port on the Microsoft SQL Server that communicates with the NA Core. In a Distributed System configuration, the SQL Server databases communicate with each other on port 1433.	Contact your Support representative for assistance.
1521	NA Core	TCP	`Oracle SQL*Net Port`	Port on the Oracle database server that communicates with the NA Core. In a Distributed System configuration, the Oracle processes connect to each other on port 1521.	Contact your Support representative for assistance.
2001	NA Satellite	TCP	`Gateway Tunnel Port`	TunnelPort from the Satellite to the Core Gateway. The Core Gateway listens for tunnel connections.	Contact your Support representative for assistance.
3002	NA Satellite	TCP	`Gateway Proxy Port`	ProxyPort from the NA Core to the Core Gateway and from the Satellite agent to the Satellite	See "Device Access Page Fields" in the NA help.
3306	NA Core	TCP	`MySQL Port`	Port on the MySQL database server that communicates with the NA Core	Contact your Support representative for assistance.
3306	NNM iSPI NET	TCP	`MySQL database port`	Provides access to MySQL database.	Change not supported.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
3873	NNMi	TCP	`nmsas.server.port.remoting.ejb3`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4040	NA Satellite	TCP	`Gateway Ident Port`	IdentPort from the NA Core to the Core Gateway	Contact your Support representative for assistance.
4444	NNMi	TCP	`nmsas.server.port.jmx.jrmp`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4445	NNMi	TCP	`nmsas.server.port.jmx.rmi`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
4446	NA Core	TCP	`jboss Remoting Port`	Port between NA clients and the NA Management Engine and between the NA Management Engines in separate NA Cores. NA clients can include: -NA Syslog Server -NA Connectors -AAA Log Reader -Syslog Reader -Customer-written API scripts (For information, see the NA API User Guide and the NA CLI/ API Command Reference.)	Contact your Support representative for assistance.
4446	NNMi	TCP	`nmsas.server.port.invoker.unified`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4457	NNMi	TCP	`nmsas.server.port.hq`	- Used for un-encrypted Global Network Management traffic. - Messaging travels from the global manager to the regional manager - Once this port is open, it becomes bi-directional	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
4459	NNMi	TCP	`nmsas.server.port.hq.ssl`	- Used for encrypted Global Network Management traffic. - Messaging travels from the global manager to the regional manager - Once this port is open, it becomes bi-directional	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4712	NA Core	TCP	`jbossTS Recovery Manager Port`	jboss transaction management	Contact your Support representative for assistance.
4712	NNMi	TCP	`nmsas.server.port.ts.recovery`	Internal transaction service port	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4713	NA Core	TCP	`jbossTS Transaction Status Manager Port`	jboss transaction management	Contact your Support representative for assistance.
4713	NNMi	TCP	`nmsas.server.port.ts.status`	Internal transaction service port	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4714	NA Core	TCP	`jbossTS Socket Process ID Port`	jboss transaction management	Contact your Support representative for assistance.
4714	NNMi	TCP	`nmsas.server.port.ts.id`	Internal transaction service port	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
5432	NNM iSPI for IP Multicast	TCP	com.hp.ov.nms.postgres.port	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
5432	NNM iSPI for IP Telephony	TCP	com.hp.ov.nms.postgres.port	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
5432	NNM iSPI for MPLS	TCP	com.hp.ov.nms.postgres.port	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
5432	NNMi	TCP	com.hp.ov.nms.postgres.port	This PostgreSQL port is the port the embedded database listens on for this NNMi management server.	Modify the %NNM_CONF%\nnm\props\nms-local.properties file (Windows) or $NNM_CONF/nnm/props/nms-local.properties file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
5432	NNM iSPI Performance for QA	TCP	`com.hp.ov.nms.postgres.port`	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
5432	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`com.hp.ov.nms.postgres.port`	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
5432	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`com.hp.ov.nms.postgres.port`	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file	N/A
5445	NA Core	TCP	`jboss HornetQ netty port`	jboss Messaging service	Contact your Support representative for assistance.
5455	NA Core	TCP	`jboss HornetQ netty-batch port`	jboss Messaging service	Contact your Support representative for assistance.
6099	NA Core	TCP	`Software Image Management Server Port`	HTTPS port from the NA server to the Software Image Management server	See "Server Page Fields" in the NA help.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
7800-7810	NNMi	TCP		- JGroups ports for application failover - If application failover is not used, HP recommends configuring the system firewall to restrict access to these ports	Modify the `%NNM_CONF%\nnm\props\nms-cluster.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-cluster.properties` file (UNIX).
8005	NA Satellite	TCP	`Tomcat Server Port`	Port for Tomcat to listen for commands like SHUTDOWN	Contact your Support representative for assistance.
8009	NA Satellite	TCP	`Tomcat AJP Port`	Port for Tomcat to listen for AJP messages	Contact your Support representative for assistance.
8022	NA Core	TCP	`SSH Server Port`	SSH port from the NA client to the NA server on the Linux or Solaris operating system	See "Telnet/SSH Page Fields" in the NA help.
8023	NA Core	TCP	`Telnet Server Port`	Telnet port from the NA client to the NA server on the Linux or Solaris operating system	See "Telnet/SSH Page Fields" in the NA help.
8080	NA Core	TCP	`HTTP Port`	HTTP port from the NA client to the NA server. Use instead of 80 when NA coexists with NNMi.	Contact your Support representative for assistance.
8080	NNM iSPI NET	TCP	`jetty http port`	Default HTTP port - used for Web UI & Web Services.	Post-install modifications not supported.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
8084	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX). You can also change this during installation.
8443	NA Core	TCP	`HTTPS Port`	HTTPS port from the NA client to the NA server. Use instead of 443 when NA coexists with NNMi.	Contact your Support representative for assistance.
8443	NA Satellite	TCP	`Tomcat HTTPS Port`	RpcPort from the Satellite to the management agent (Tomcat), Syslog, TFTP	Contact your Support representative for assistance.
8443	NNM iSPI NET	TCP	`jetty SSL/https port`	Default HTTPS port - used for Web UI & Web Services.	Post-install modifications not supported.
8886	NNMi	TCP	`OVsPMD_MGMT`	NNMi `ovspmd` (process manager) management port	Modify the `/etc/services` file
8887	NNMi	TCP	`OVsPMD_REQ`	NNMi `ovsmpd` (process manager) request port	Modify the `/etc/services` file
9004	NNM iSPI NET	TCP	`HP OO RAS port`	Provides access to HP OO Remote Action Service.	Change not supported.
9090	NA Satellite	TCP	`Gateway Admin Port`	AdminPort from the Satellite to the Core Gateway. Note that the Satellite uses all of the ports that the NA Core uses for managing devices (from the Satellite to the device: 22, 23, 514, 80, and 443).	See "Device Access Page Fields" in the NA help.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
9300	NNM iSPI Performance for Metrics and NPS	TCP	NPS UI	Default HTTP port - used for Web UI & BI Web Services.	Change using configureWebAccess.ovpl.
9301	NNM iSPI Performance for Metrics and NPS	TCP	Sybase ASE	Sybase ASE (BI Content Manager Database). Used by processes running on the same server.	Change not supported.
9302	NNM iSPI Performance for Metrics and NPS	TCP	Sybase IQ Agent	Sybase IQ Agent service. Used by processes running on the same server.	Change not supported.
9303	NNM iSPI Performance for Metrics and NPS	TCP	Sybase IQ - PerfSPI DB	Sybase IQ database used to store all NPS extensionPack data. Used by processes running on the same server.	Change not supported.
9304	NNM iSPI Performance for Metrics and NPS	TCP	Sybase IQ - PerfSPI **DEMO DB**	Sybase IQ database used to store extensionPack **DEMO** data. Used by processes running on the same server.	Change not supported.
9305	NNM iSPI Performance for Metrics and NPS	TCP	NPS UI - SSL	Default Secure HTTPS port (SSL) - used for Web UI & BI Web Services.	Change using configureWebAccess.ovpl.
9306	NNM iSPI Performance for Metrics and NPS	TCP	Database SQL Rewrite Proxy - PerfSPI DB	SQL Rewrite proxy for the Perfspi database - used by BI Server. Used by processes running on the same server.	Change not supported.
9307	NNM iSPI Performance for Metrics and NPS	TCP	Database SQL Rewrite Proxy - PerfSPI **DEMO DB**	SQL Rewrite proxy for the Perfspi **DEMO** database - used by BI Server. Used by processes running on the same server.	Change not supported.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
9308	NNM iSPI Performance for Metrics and NPS	TCP	`Sybase ASE Backup Server`	Sybase ASE backup server for the BI content manager database. Used by processes running on the same server.	Change not supported.
10080	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX). You can also change this during installation.
10083	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10084	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10085	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
10086	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10087	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10089	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10092	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10099	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX). You can also change this during installation.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
10443	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX). You can also change this during installation.
11080	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX). You can also change this during installation.
11081	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX). You can also change this during installation.
11083	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
11084	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11085	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11086	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11087	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11089	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
11092	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11099	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX). You can also change this during installation.
11712	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11713	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11714	NNM iSPI Performance for Traffic (Traffic Leaf)	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
12080	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX). You can also change this during installation.
12081	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX). You can also change this during installation.
12083	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12084	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
12085	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12086	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12087	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12089	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12092	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
12099	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX). You can also change this during installation.
12712	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12713	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12714	NNM iSPI Performance for Traffic (Traffic Master)	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
14083	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
14084	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14085	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14086	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14087	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14089	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
14092	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14099	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX). You can also change this during installation.
14102	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14103	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14104	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
14443	NNM iSPI for IP Multicast	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX). You can also change this during installation.
14712	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
14713	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
14714	NNM iSPI for IP Telephony	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
24040	NNM iSPI for MPLS	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX). You can also change this during installation.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
24041	NNM iSPI for MPLS	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24043	NNM iSPI for MPLS	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX). You can also change this during installation.
24044	NNM iSPI for MPLS	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24045	NNM iSPI for MPLS	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
24046	NNM iSPI for MPLS	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX). You can also change this during installation.
24047	NNM iSPI for MPLS	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24048	NNM iSPI for MPLS	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24049	NNM iSPI for MPLS	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24092	NNM iSPI for MPLS	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
24712	NNM iSPI for MPLS	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24713	NNM iSPI for MPLS	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24714	NNM iSPI for MPLS	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
54040	NNM iSPI Performance for QA	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX). You can also change this during installation.
54043	NNM iSPI Performance for QA	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX). You can also change this during installation.

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
54046	NNM iSPI Performance for QA	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX). You can also change this during installation.
54047	NNM iSPI Performance for QA	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54084	NNM iSPI Performance for QA	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54085	NNM iSPI Performance for QA	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54086	NNM iSPI Performance for QA	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
54087	NNM iSPI Performance for QA	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54088	NNM iSPI Performance for QA	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54089	NNM iSPI Performance for QA	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).

Table 2 Ports Used by NMC Products (cont'd)

Port	NMC Product	Type	Name	Purpose	Change Configuration
54712	NNM iSPI Performance for QA	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54713	NNM iSPI Performance for QA	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54714	NNM iSPI Performance for QA	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).

HP Network Node Manager i Software

Table 3 shows the ports NNMi uses on the management server. NNMi listens on these ports. If port conflicts occur, you can change most of these port numbers as shown in the *Change Configuration* column. See the *nnm.ports* reference page, or the UNIX manpage, for more information.

For application failover to work successfully, open TCP ports 7800-7810. For the application failover feature to function correctly, the active and standby NNMi management servers must have unrestricted network access to each other.

Table 3 Ports Used on the NNMi Management Server

Port	Type	Name	Purpose	Change Configuration
80	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI & Web Services - In GNM configurations NNMi uses this port to establish communication from the global manager to the regional manager - Once this port is open, it becomes bi-directional	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX). You can also change this during installation.
162	UDP	`trapPort`	SNMP trap port	Modify using the `nnmtrapconfig.ovpl` Perl script. See the *nnmtrapconfig.ovpl* reference page, or the UNIX manpage, for more information.
443	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI & Web Services	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
1098	TCP	`nmsas.server.port.naming.rmi`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).

Table 3 Ports Used on the NNMi Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
1099	TCP	`nmsas.server.port.naming.port`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
3873	TCP	`nmsas.server.port.remoting.ejb3`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4444	TCP	`nmsas.server.port.jmx.jrmp`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4445	TCP	`nmsas.server.port.jmx.rmi`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4446	TCP	`nmsas.server.port.invoker.unified`	- Used by NNMi command line tools to communicate with a variety of services used by NNMi - HP recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).
4457	TCP	`nmsas.server.port.hq`	- Used for un-encrypted Global Network Management traffic. - Messaging travels from the global manager to the regional manager - Once this port is open, it becomes bi-directional	Modify the `%NNM_CONF%\nnm\props\nms-local.properties` file (Windows) or `$NNM_CONF/nnm/props/nms-local.properties` file (UNIX).

Table 3 Ports Used on the NNMi Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
4459	TCP	nmsas.server.port.hq.ssl	- Used for encrypted Global Network Management traffic. - Messaging travels from the global manager to the regional manager - Once this port is open, it becomes bi-directional	Modify the %NNM_CONF%\nnm\props\nms-local.properties file (Windows) or $NNM_CONF/nnm/props/nms-local.properties file (UNIX).
4712	TCP	nmsas.server.port.ts.recovery	Internal transaction service port	Modify the %NNM_CONF%\nnm\props\nms-local.properties file (Windows) or $NNM_CONF/nnm/props/nms-local.properties file (UNIX).
4713	TCP	nmsas.server.port.ts.status	Internal transaction service port	Modify the %NNM_CONF%\nnm\props\nms-local.properties file (Windows) or $NNM_CONF/nnm/props/nms-local.properties file (UNIX).
4714	TCP	nmsas.server.port.ts.id	Internal transaction service port	Modify the %NNM_CONF%\nnm\props\nms-local.properties file (Windows) or $NNM_CONF/nnm/props/nms-local.properties file (UNIX).
5432	TCP	com.hp.ov.nms.postgres.port	This PostgreSQL port is the port the embedded database listens on for this NNMi management server.	Modify the %NNM_CONF%\nnm\props\nms-local.properties file (Windows) or $NNM_CONF/nnm/props/nms-local.properties file (UNIX).
7800-7810	TCP		- JGroups ports for application failover - If application failover is not used, HP recommends configuring the system firewall to restrict access to these ports	Modify the %NNM_CONF%\nnm\props\nms-cluster.properties file (Windows) or $NNM_CONF/nnm/props/nms-cluster.properties file (UNIX).
8886	TCP	OVsPMD_MGMT	NNMi ovspmd (process manager) management port	Modify the /etc/services file
8887	TCP	OVsPMD_REQ	NNMi ovsmpd (process manager) request port	Modify the /etc/services file

Table 4 shows some of the ports NNMi uses to communicate with other systems. If a firewall separates NNMi from these systems, you must open many of these ports in the firewall. The actual set of ports depends on the set of integrations you configured to use with NNMi and how you configured those integrations. If column 4 indicates *Client*, NNMi connects or sends to this port; if column 4 indicates *Server*, NNMi listens on this port.

Table 4 Ports Used for Communication Between the NNMi Management Server and Other Systems

Port	Type	Purpose	Client, Server
80	TCP	Default HTTP port for NNMi; used for Web UI and Web Services	Server
80	TCP	Default HTTP port for NNMi connecting to other applications. The actual port depends on NNMi configuration.	Client
161	UDP	SNMP request port	Client
162	UDP	SNMP trap port - traps received by NNMi	Server
162	UDP	SNMP trap port; Trap Forwarding, Northbound Interface, or NetCool integrations	Client
389	TCP	Default LDAP port	Client
395	UDP	nGenius Probe SNMP trap port	Client
443	TCP	Default secure HTTPS port for NNMi connecting to other applications; the actual port depends onNNMi configuration. Default HTTPS port for HP OM on Windows	Client
443	TCP	Default secure HTTPS port; used for Web UI and Web Services	Server
636	TCP	Default secure LDAP port (SSL)	Client
1741	TCP	Default CiscoWorks LMS web services port	Client
4457	TCP	Used for un-encrypted Global Network Management traffic. The connection is from the global manager to the regional manager.	Client, Server
4459	TCP	Used for encrypted Global Network Management traffic. The connection is from the global manager to the regional manager.	Client, Server
7800-7810	TCP	JGroups ports for application failover	Client and Server
8004	TCP	Default HTTP port for NNMi if another web server already has port 80. Used for Web UI and Web Services. Verify the actual HTTP port for your NNMi management server.	Server
8080	TCP	Default HTTP port for connecting to NA if installed on the same system as NNMi. Default HTTPS port for HP UCMDB web services	Client
8443 or 8444	TCP	Default HTTP port for connecting to HP OM for UNIX	Client
9300	TCP	Default HTTP port for connecting to NNM iSPI Performance for Metrics	Client
50000	TCP	Default HTTPS port for connecting to SIM	Client

If you configure NNMi to use ICMP fault polling or ping sweep for discovery, configure the firewall to pass ICMP packets through the firewall.

The Web Services approach for the NNMi-HP OM integration does not work through a firewall, however the NNMi-HP OM integration using the Northbound Interface does work through a firewall.

If you plan to use the global network management feature, Table 5 shows the well-known ports that need to be accessible from a global NNMi management server to a regional NNMi management server. The global network management feature requires these ports to be open for TCP access from the global NNMi management server to the regional NNMi management server. The regional NNMi management server will not open sockets back to the global NNMi management server.

Table 5 Required Accessible Sockets for Global Network Management

Security	Parameter	TCP Port
non-SSL	jboss.http.port	80
	jboss.bisocket.port	4457
SSL	jboss.https.port	443
	jboss.sslbisocket.port	4459

NNM iSPI for MPLS

Table 6 shows the ports the HP Network Node Manager iSPI for MPLS Software uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the server.properties file located at: `%NnmDataDir%/nmsas/mpls/server.properties`.

Table 6 Ports Used on the HP Network Node Manager iSPI for MPLS Software Management Server

Port	Type	Name	Purpose	Change Configuration
5432	TCP	`com.hp.ov.nms.postgres.port`	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
24040	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX). You can also change this during installation.
24041	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24043	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX). You can also change this during installation.

Table 6 Ports Used on the HP Network Node Manager iSPI for MPLS Software Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
24044	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24045	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24046	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX). You can also change this during installation.
24047	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24048	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).

Table 6 Ports Used on the HP Network Node Manager iSPI for MPLS Software Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
24049	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24092	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24712	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24713	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).
24714	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\mpls\server.properties` file (Windows) or `$NnmDataDir/nmsas/mpls/server.properties` file (UNIX).

NNM iSPI for IP Telephony

Table 7 shows the ports the NNM iSPI for IP Telephony uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the server.properties file located at: `%NnmDataDir%/nmsas/ipt/server.properties`.

Table 7 Ports Used on the NNM iSPI for IP Telephony Management Server

Port	Type	Name	Purpose	Change Configuration
5432	TCP	`com.hp.ov.nms.postgres.port`	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
10080	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX). You can also change this during installation.
10083	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10084	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).

Table 7 Ports Used on the NNM iSPI for IP Telephony Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
10085	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10086	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10087	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10089	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
10092	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).

Table 7 Ports Used on the NNM iSPI for IP Telephony Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
10099	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX). You can also change this during installation.
10443	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX). You can also change this during installation.
14712	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
14713	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).
14714	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\ipt\server.properties` file (Windows) or `$NnmDataDir/nmsas/ipt/server.properties` file (UNIX).

NNM iSPI for IP Multicast

Table 8 shows the ports the NNM iSPI for IP Multicast uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the server.properties file located at: `%NnmDataDir%/nmsas/multicast/server.properties`.

Table 8 Ports Used on the NNM iSPI for IP Multicast Management Server

Port	Type	Name	Purpose	Change Configuration
5432	TCP	`com.hp.ov.nms.postgres.port`	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
8084	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX). You can also change this during installation.
14083	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14084	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).

Table 8 Ports Used on the NNM iSPI for IP Multicast Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
14085	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14086	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14087	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14089	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).
14092	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\multicast\server.properties` file (Windows) or `$NnmDataDir/nmsas/multicast/server.properties` file (UNIX).

Table 8 Ports Used on the NNM iSPI for IP Multicast Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
14099	TCP	nmsas.server.port.naming.port	Default bootstrap JNP service port (JNDI provider)	Modify the %NnmDataDir%\nmsas\multicast\server.properties file (Windows) or $NnmDataDir/nmsas/multicast/server.properties file (UNIX). You can also change this during installation.
14102	TCP	nmsas.server.port.ts.id	Default port used by the Transaction service.	Modify the %NnmDataDir%\nmsas\multicast\server.properties file (Windows) or $NnmDataDir/nmsas/multicast/server.properties file (UNIX).
14103	TCP	nmsas.server.port.ts.recovery	Default recovery port used by the Transaction service.	Modify the %NnmDataDir%\nmsas\multicast\server.properties file (Windows) or $NnmDataDir/nmsas/multicast/server.properties file (UNIX).
14104	TCP	nmsas.server.port.ts.status	Default status port used by the Transaction service.	Modify the %NnmDataDir%\nmsas\multicast\server.properties file (Windows) or $NnmDataDir/nmsas/multicast/server.properties file (UNIX).
14443	TCP	nmsas.server.port.web.https	Default secure HTTPS port (SSL) - used for Web UI.	Modify the %NnmDataDir%\nmsas\multicast\server.properties file (Windows) or $NnmDataDir/nmsas/multicast/server.properties file (UNIX). You can also change this during installation.

NNM iSPI Performance for Traffic

Table 9 shows the ports the NNM iSPI Performance for Traffic (Traffic Master component) uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the server.properties file located at: `%NnmDataDir%/nmsas/traffic-master/server.properties`.

Table 9 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Master)

Port	Type	Name	Purpose	Change Configuration
5432	TCP	`com.hp.ov.nms.postgres.port`	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file	N/A
12080	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX). You can also change this during installation.
12081	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX). You can also change this during installation.
12083	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).

Table 9 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Master) (cont'd)

Port	Type	Name	Purpose	Change Configuration
12084	TCP	nmsas.server.port.jmx.jrmp	Default RMI object port (JRMP invoker)	Modify the %NnmDataDir%\nmsas\traffic-master\server.properties file (Windows) or $NnmDataDir/nmsas/traffic-master/server.properties file (UNIX).
12085	TCP	nmsas.server.port.jmx.rmi	Default RMI pooled invoker port	Modify the %NnmDataDir%\nmsas\traffic-master\server.properties file (Windows) or $NnmDataDir/nmsas/traffic-master/server.properties file (UNIX).
12086	TCP	nmsas.server.port.invoker.unified	Default RMI remoting server connector port	Modify the %NnmDataDir%\nmsas\traffic-master\server.properties file (Windows) or $NnmDataDir/nmsas/traffic-master/server.properties file (UNIX).
12087	TCP	nmsas.server.port.hq	Used for un-encrypted Global Network Management traffic.	Modify the %NnmDataDir%\nmsas\traffic-master\server.properties file (Windows) or $NnmDataDir/nmsas/traffic-master/server.properties file (UNIX).
12089	TCP	nmsas.server.port.remoting.ejb3	Default EJB3	Modify the %NnmDataDir%\nmsas\traffic-master\server.properties file (Windows) or $NnmDataDir/nmsas/traffic-master/server.properties file (UNIX).

Table 9 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Master) (cont'd)

Port	Type	Name	Purpose	Change Configuration
12092	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12099	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX). You can also change this during installation.
12712	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12713	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).
12714	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-master\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-master/server.properties` file (UNIX).

Table 10 shows the ports the NNM iSPI Performance for Traffic (Traffic Leaf component) uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the server.properties file located at: `%NnmDataDir%/nmsas/traffic-leaf/server.properties`.

Table 10 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Leaf)

Port	Type	Name	Purpose	Change Configuration
5432	TCP	`com.hp.ov.nms.postgres.port`	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
11080	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX). You can also change this during installation.
11081	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX). You can also change this during installation.
11083	TCP	`nmsas.server.port.naming.rmi`	Default port for RMI naming service	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).

Table 10 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Leaf) (cont'd)

Port	Type	Name	Purpose	Change Configuration
11084	TCP	`nmsas.server.port.jmx.jrmp`	Default RMI object port (JRMP invoker)	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11085	TCP	`nmsas.server.port.jmx.rmi`	Default RMI pooled invoker port	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11086	TCP	`nmsas.server.port.invoker.unified`	Default RMI remoting server connector port	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11087	TCP	`nmsas.server.port.hq`	Used for un-encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11089	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).

Table 10 Ports Used on the NNM iSPI Performance for Traffic Management Server (Traffic Leaf) (cont'd)

Port	Type	Name	Purpose	Change Configuration
11092	TCP	`nmsas.server.port.hq.ssl`	Used for encrypted Global Network Management traffic.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11099	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX). You can also change this during installation.
11712	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11713	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).
11714	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\traffic-leaf\server.properties` file (Windows) or `$NnmDataDir/nmsas/traffic-leaf/server.properties` file (UNIX).

NNM iSPI Performance for QA

Table 11 shows the ports theNNM iSPI Performance for QA uses on the management server. In case of port conflicts, almost all of these port numbers can be changed using the server.properties file located at: `%NnmDataDir%/nmsas/qa/server.properties`.

Table 11 Ports Used on the NNM iSPI Performance for QA Management Server

Port	Type	Name	Purpose	Change Configuration
5432	TCP	`com.hp.ov.nms.postgres.port`	This PostgreSQL port is the port the embedded database listens on for this NNMi management server. The port is expected to be the same as that configured for NNMi in the nms-local.properties file.	N/A
54040	TCP	`nmsas.server.port.web.http`	Default HTTP port - used for Web UI.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX). You can also change this during installation.
54043	TCP	`nmsas.server.port.web.https`	Default secure HTTPS port (SSL) - used for Web UI.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX). You can also change this during installation.
54046	TCP	`nmsas.server.port.naming.port`	Default bootstrap JNP service port (JNDI provider)	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX). You can also change this during installation.

Table 11 Ports Used on the NNM iSPI Performance for QA Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
54047	TCP	nmsas.server.port.naming.rmi	Default port for RMI naming service	Modify the %NnmDataDir%\nmsas\qa\server.properties file (Windows) or $NnmDataDir/nmsas/qa/server.properties file (UNIX).
54084	TCP	nmsas.server.port.jmx.jrmp	Default RMI object port (JRMP invoker)	Modify the %NnmDataDir%\nmsas\qa\server.properties file (Windows) or $NnmDataDir/nmsas/qa/server.properties file (UNIX).
54085	TCP	nmsas.server.port.jmx.rmi	Default RMI pooled invoker port	Modify the %NnmDataDir%\nmsas\qa\server.properties file (Windows) or $NnmDataDir/nmsas/qa/server.properties file (UNIX).
54086	TCP	nmsas.server.port.invoker.unified	Default RMI remoting server connector port	Modify the %NnmDataDir%\nmsas\qa\server.properties file (Windows) or $NnmDataDir/nmsas/qa/server.properties file (UNIX).
54087	TCP	nmsas.server.port.hq	Used for un-encrypted Global Network Management traffic.	Modify the %NnmDataDir%\nmsas\qa\server.properties file (Windows) or $NnmDataDir/nmsas/qa/server.properties file (UNIX).
54088	TCP	nmsas.server.port.hq.ssl	Used for encrypted Global Network Management traffic.	Modify the %NnmDataDir%\nmsas\qa\server.properties file (Windows) or $NnmDataDir/nmsas/qa/server.properties file (UNIX).

Table 11 Ports Used on the NNM iSPI Performance for QA Management Server (cont'd)

Port	Type	Name	Purpose	Change Configuration
54089	TCP	`nmsas.server.port.remoting.ejb3`	Default EJB3 remoting connector port	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54712	TCP	`nmsas.server.port.ts.recovery`	Default recovery port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54713	TCP	`nmsas.server.port.ts.status`	Default status port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).
54714	TCP	`nmsas.server.port.ts.id`	Default port used by the Transaction service.	Modify the `%NnmDataDir%\nmsas\qa\server.properties` file (Windows) or `$NnmDataDir/nmsas/qa/server.properties` file (UNIX).

NNM iSPI Performance for Metrics and NPS

Table 12 shows the ports required for NNM iSPI Performance for Metrics and Network Performance Server (NPS). In case of port conflicts, almost all of these port numbers can be changed.

If NNMi and NPS are not coexisting, then the network ports used for the OS network file sharing are also required (NFS services on Linux, Windows File Sharing on Windows).

Table 12 Required Ports for NNM iSPI Performance for Metrics and NPS

Port	Type	Name	Purpose	Change Configuration
9300	TCP	NPS UI	Default HTTP port - used for Web UI & BI Web Services.	Change using configureWebAccess.ovpl.
9301	TCP	Sybase ASE	Sybase ASE (BI Content Manager Database). Used by processes running on the same server.	Change not supported.
9302	TCP	Sybase IQ Agent	Sybase IQ Agent service. Used by processes running on the same server.	Change not supported.
9303	TCP	Sybase IQ - PerfSPI DB	Sybase IQ database used to store all NPS extensionPack data. Used by processes running on the same server.	Change not supported.
9304	TCP	Sybase IQ - PerfSPI **DEMO DB**	Sybase IQ database used to store extensionPack **DEMO** data. Used by processes running on the same server.	Change not supported.
9305	TCP	NPS UI - SSL	Default Secure HTTPS port (SSL) - used for Web UI & BI Web Services.	Change using configureWebAccess.ovpl.
9306	TCP	Database SQL Rewrite Proxy - PerfSPI DB	SQL Rewrite proxy for the Perfspi database - used by BI Server. Used by processes running on the same server.	Change not supported.
9307	TCP	Database SQL Rewrite Proxy - PerfSPI **DEMO DB**	SQL Rewrite proxy for the Perfspi **DEMO** database - used by BI Server. Used by processes running on the same server.	Change not supported.
9308	TCP	Sybase ASE Backup Server	Sybase ASE backup server for the BI content manager database. Used by processes running on the same server.	Change not supported.

NNM iSPI NET

Table 13 shows the ports used by the NNM iSPI NET diagnostics server. The NNM iSPI NET diagnostic server installs HP Operations Orchestration (HP OO). For more information, see the *HP Operations Orchestration Administrator's Guide*.

Table 13 Ports Used by the NNM iSPI NET Diagnostics Server

Port	Type	Name	Purpose	Change Configuration
3306	TCP	`MySQL database port`	Provides access to MySQL database.	Change not supported.
8080	TCP	`jetty http port`	Default HTTP port - used for Web UI & Web Services.	Post-install modifications not supported.
8443	TCP	`jetty SSL/https port`	Default HTTPS port - used for Web UI & Web Services.	Post-install modifications not supported.
9004	TCP	`HP OO RAS port`	Provides access to HP OO Remote Action Service.	Change not supported.

HP Network Automation

Table 14 shows the ports used by HP Network Automation (NA Core).

Table 14 Ports Used by HP Network Automation (NA Core)

Port	Type	Name	Purpose	Change Configuration
22	TCP	SSH Server Port	SSH port from the NA client to the NA server on the Windows operating system	See "Telnet/SSH Page Fields" in the NA help.
23	TCP	Telnet Server Port	Telnet port from the NA client to the NA server on the Windows operating system	See "Telnet/SSH Page Fields" in the NA help.
69	UDP	TFTP Port	Network devices to the NA server	Change not supported
80	TCP	HTTP Port	HTTP port from the NA client to the NA server	Contact your Support representative for assistance.
443	TCP	HTTPS Port	HTTPS port from the NA client to the NA server	Contact your Support representative for assistance.
514	UDP	Syslog Port	Receive syslog messages from network devices on the NA server	See “Configuring the NA Syslog Server” in the NA Installation and Upgrade Guide.
1098	TCP	RMI Activation Port	Port between NA clients and the NA Management Engine and between the NA Management Engines in separate NA Cores. NA clients can include: -NA Syslog Server -NA Connectors -AAA Log Reader -Syslog Reader -Customer-written API scripts (For information, see the NA API User Guide and the NA CLI/API Command Reference.)	Contact your Support representative for assistance.

Table 14 Ports Used by HP Network Automation (NA Core) (cont'd)

Port	Type	Name	Purpose	Change Configuration
1099	TCP	RMI Registration Port	Port between NA clients and the NA Management Engine and between the NA Management Engines in separate NA Cores. NA clients can include: -NA Syslog Server -NA Connectors -AAA Log Reader -Syslog Reader -Customer-written API scripts (For information, see the NA API User Guide and the NA CLI/API Command Reference.)	Contact your Support representative for assistance.
1433	TCP	Microsoft SQL Server Port	Port on the Microsoft SQL Server that communicates with the NA Core. In a Distributed System configuration, the SQL Server databases communicate with each other on port 1433.	Contact your Support representative for assistance.
1521	TCP	Oracle SQL*Net Port	Port on the Oracle database server that communicates with the NA Core. In a Distributed System configuration, the Oracle processes connect to each other on port 1521.	Contact your Support representative for assistance.
3306	TCP	MySQL Port	Port on the MySQL database server that communicates with the NA Core	Contact your Support representative for assistance.
4446	TCP	jboss Remoting Port	Port between NA clients and the NA Management Engine and between the NA Management Engines in separate NA Cores. NA clients can include: -NA Syslog Server -NA Connectors -AAA Log Reader -Syslog Reader -Customer-written API scripts (For information, see the NA API User Guide and the NA CLI/API Command Reference.)	Contact your Support representative for assistance.
4712	TCP	jbossTS Recovery Manager Port	jboss transaction management	Contact your Support representative for assistance.

Table 14 Ports Used by HP Network Automation (NA Core) (cont'd)

Port	Type	Name	Purpose	Change Configuration
4713	TCP	`jbossTS Transaction Status Manager Port`	jboss transaction management	Contact your Support representative for assistance.
4714	TCP	`jbossTS Socket Process ID Port`	jboss transaction management	Contact your Support representative for assistance.
5445	TCP	`jboss HornetQ netty port`	jboss Messaging service	Contact your Support representative for assistance.
5455	TCP	`jboss HornetQ netty-batch port`	jboss Messaging service	Contact your Support representative for assistance.
6099	TCP	`Software Image Management Server Port`	HTTPS port from the NA server to the Software Image Management server	See "Server Page Fields" in the NA help.
8022	TCP	`SSH Server Port`	SSH port from the NA client to the NA server on the Linux or Solaris operating system	See "Telnet/SSH Page Fields" in the NA help.
8023	TCP	`Telnet Server Port`	Telnet port from the NA client to the NA server on the Linux or Solaris operating system	See "Telnet/SSH Page Fields" in the NA help.
8080	TCP	`HTTP Port`	HTTP port from the NA client to the NA server. Use instead of 80 when NA coexists with NNMi.	Contact your Support representative for assistance.
8443	TCP	`HTTPS Port`	HTTPS port from the NA client to the NA server. Use instead of 443 when NA coexists with NNMi.	Contact your Support representative for assistance.

Table 15 shows the ports used by HP Network Automation (NA Satellite).

Table 15 Ports Used by HP Network Automation (NA Satellite)

Port	Type	Name	Purpose	Change Configuration
2001	TCP	Gateway Tunnel Port	TunnelPort from the Satellite to the Core Gateway. The Core Gateway listens for tunnel connections.	Contact your Support representative for assistance.
3002	TCP	Gateway Proxy Port	ProxyPort from the NA Core to the Core Gateway and from the Satellite agent to the Satellite	See "Device Access Page Fields" in the NA help.
4040	TCP	Gateway Ident Port	IdentPort from the NA Core to the Core Gateway	Contact your Support representative for assistance.
8005	TCP	Tomcat Server Port	Port for Tomcat to listen for commands like SHUTDOWN	Contact your Support representative for assistance.
8009	TCP	Tomcat AJP Port	Port for Tomcat to listen for AJP messages	Contact your Support representative for assistance.
8443	TCP	Tomcat HTTPS Port	RpcPort from the Satellite to the management agent (Tomcat), Syslog, TFTP	Contact your Support representative for assistance.
9090	TCP	Gateway Admin Port	AdminPort from the Satellite to the Core Gateway. Note that the Satellite uses all of the ports that the NA Core uses for managing devices (from the Satellite to the device: 22, 23, 514, 80, and 443).	See "Device Access Page Fields" in the NA help.

4 IPv6 Readiness

HP Network Automation (NA) is a robust network element management and automation tool. NA communicates with network elements via numerous protocols and authentication methods to gather information. NA then parses the information, normalizing it in a searchable and presentable format.

NA supports IPv6, both as transport and as parsed searchable and presentable bits of IPv6 specific information. NA supports IPv6 connections to DBMS. This includes Microsoft SQL Server 2005.

NA's adoption of IPv6 is focused on providing:

- Transparent access to network elements via IPv4 and/or IPv6
- Information on network element IPv6 configurations
- IPv6 support across NA features

Installation

NA installs and automatically detects network provisioning on the server. The available protocol determines what protocol NA uses for communicating to elements and NA listening servers. This includes:

- IPv4 only
- IPv6 only
- Dual stack environments (whether native or using a transition mechanism)

If NA is installed on a server that is to be updated to support IPv6, the following procedure is recommended:

1. Shut down NA.
2. Add IPv6 support to the server.
3. Restart NA.
4. Check the Admin options for various servers to ensure correct IPv6 address discovery.

Network Services

NA has several network services that will appropriately listen on IPv4-only, IPv6-only, and dual stack environments. These include:

- Web Server (TCP 80 and 443) — Clients using IPv6-enabled OS and browser can access NA via IPv6.
- TFTP Server (UDP 69) — Network elements can upload/download information via TFTP IPv6.
- TELNET Server (TCP 23) — Network elements can upload/download information via TELNET IPv6. Clients accessing the NA CLI can do it via TELNET IPv6.
- SSH/SCP Server (TCP 22) — Network elements can upload/download information via SSH/SCP IPv6. Clients accessing the NA CLI can do it via SSH IPv6.
- SYSLOG Server (UDP 514) — Network elements reporting change can do it via SYSLOG IPv6.

NA functions that instruct network elements to access these services will correctly determine which protocol to use based on a number of factors.

Clients

NA uses numerous protocols for intra-communication and communicating with network elements. These include:

- HTTP (TCP 80) — Access network elements
- HTTP (TCP 443) — Access network elements
- FTP (TCP 21) — Access network elements
- SNMP (UDP 161) — Access network elements
- Telnet (TCP 23) — Access network elements
- SSH/SCP (TCP 22) — Access network elements
- SYSLOG (UDP 514) — Send logging message
- SMTP (TCP 25) — Send email

IPv6 Presentation

The NA user interface supports IPv6 notation. This includes correct understanding, parsing, input, and display of IPv6 addresses. NA provides unique searching features for searching for IPv6 addresses within the system.

NA Features Supporting IPv6

The following NA features support IPv6:

- Detect Network Device
- Discover Driver
- Device Reservation
- Take Snapshot
- Configure Syslog
- Deploy Passwords
- Reboot Device
- Run Command Script
- Run Diagnostics
- Synchronize Startup and Running
- Update Device Software
- Import
- Deduplication
- Check Policy Compliance
- Resolve FQDN
- Searching
- Reporting
- Real time change management
- Work Flow
- CLI and API

Drivers

NA architecture is such that a driver layer exists between the NA Core and the managed network elements. This layer abstracts information from network elements, interprets it, and then forwards the information to NA. NA has IPv6 driver dependencies. As a result, not all drivers support all features of IPv6. Primary adoption includes the Cisco family of network elements.

Currently, the following NA components do not support IPv6:

- Overlapping IPs — Satellite Gateways do not support IPv6.
- Dynamic IPv6 addresses — NA does not gather or track information on device elements or dynamically assigned IPv6 addresses (for example, link local and multicast).
- IPv6 ACLs — The ACL specific feature does not parse/process IPv6 ACLs, though functionality to search, add, delete, and edit IPv6 ACLs exists.
- NMAP — Using NMAP with the NA Detect Network Device feature do not work.
- Multimaster Distributed System and Horizontal Scalability — Dual stack is supported, however with the replication/RMI using IPv4-only.
- Topology Diagramming — Topology diagramming does not support IPv6.
- SA/NA integration — HP Server Automaton does not support IPv6.
- OO/NA integration — HP Operations Orchestration does not support IPv6.

- NNMi/NA integration- HP Network Node Manager with dual stack is supported, but not with IPv6-only.
- BSAE/NA integration — Business Service Automaton Essentials does not support IPv6.
- DDS integration — The Driver Delivery System does not support IPv6.

5 Tuning NA Performance

This chapter describes several ways to tune the performance of HP Network Automation Software (NA). It includes the following topics:

Tuning the NA Management Engine

This section describes recommended tuning of the NA Management Engine. If you update the maximum number of concurrent tasks, also update the maximum data source pool size and the number of connections from NA to the Oracle database.

Task Scheduling

It is recommended that scheduled tasks be plan to run throughout the day to balance the use of NA server resources.

It is recommend that snapshot tasks occur after the work day ends to capture that day's changes.

Maximum Concurrent Tasks

The maximum number of concurrent tasks tunes the NA task functionality.

The recommended value for the maximum number of concurrent tasks depends on the size of the NA deployment, as described in "Tuning Settings" in the *NA Support Matrix*. A higher value is not necessarily better.

To set the maximum number of concurrent tasks, follow these steps:

1. Log on to the NA console as an NA administrator.
2. On the Administrative Settings - Server page (**Admin > Administrative Settings > Server**), under Tasks, set Max Concurrent Tasks to the value recommended in "Tuning Settings" in the *NA Support Matrix*, and then click **Save**.

After changing the maximum number of concurrent tasks, see Maximum Data Source Pool Size on page 78 and Number of Database Connections from NA on page 81.

Maximum Data Source Pool Size

If you change the Max Concurrent Tasks setting or the Max Concurrent Group Tasks setting or if the expected maximum number of concurrent users of the NA console changes considerably, update the maximum data source pool size configuration.

The correct maximum data source pool size is the sum of the following factors:

- The Max Concurrent Tasks setting

  This value is listed under Tasks on the Administrative Settings - Server page.

- The Max Concurrent Group Tasks setting

  This value is listed under Tasks on the Administrative Settings - Server page.

- The expected maximum number of concurrent NA users

  This number depends on the way your company uses NA.

  The All Users page (**Admin >Users**) lists all user accounts that can connect to NA.

- A buffer of 20

To set the maximum data source pool size configuration, follow these steps:

1. Stop all NA services.
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

     ```
     /etc/init.d/truecontrol stop
     ```

2. To set the maximum data source pool size value, do the following:
   a. Change to the following directory:
      - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\deploy`
      - *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/deploy`
   b. Back up the `db-ds.xml` file to a location outside the `<NA_HOME>` directory.
   c. In a text editor such as WordPad or vi, open the `db-ds.xml` file.
   d. Search for the string `NASDataSource` to locate the following lines:

      ```
      <attribute name="DataSourceName">NASDataSource</attribute>
      <attribute name="InitialPoolSize">0</attribute>
      <attribute name="MinPoolSize">0</attribute>
      <attribute name="MaxPoolSize">50</attribute>
      ```

   e. Set the `MaxPoolSize` attribute to the calculated value.

f Search for the string `NASReportDataSource` to locate the following lines:

```
<attribute name="DataSourceName">NASReportDataSource</attribute>
<attribute name="InitialPoolSize">0</attribute>
<attribute name="MinPoolSize">0</attribute>
<attribute name="MaxPoolSize">50</attribute>
```

g Identify, but do *not* change, the value of the the `MaxPoolSize` attribute for the NA report data source configuration.

The values of both maximum pool size attributes factor into the calculation of the number of available database connections.

h Save the `db-ds.xml` file.

3 In an NA Horizontal Scalability environment, repeat step 2 on each NA server.

4 On each NA server, start all NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  `/etc/init.d/truecontrol start`
-

Configuring the Java Virtual Machine

The recommended configuration of the Java virtual machine (JVM) heap and young generation sizes depend on the size of the NA deployment, as described in "Tuning Settings" in the *NA Support Matrix*.

The JVM configuration is specified in megabytes.

To set the JVM heap and young generation size, follow these steps:

1 Change to the directory that contains the JVM configuration files:

- *Windows*: `<HA_HOME>\server\ext\wrapper\conf`
- *UNIX*: `<HA_HOME>/server/ext/wrapper/conf`

2 Back up the `jboss_wrapper.conf` file to a location outside the `<NA_HOME>` directory.

3 In a text editor such as WordPad or vi, open the `jboss_wrapper.conf` file.

4 Search for the string `initmemory` to locate the lines similar to the following lines:

```
# Initial Java Heap Size (in MB)
wrapper.java.initmemory=8192
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=8192
```

5 Compare the values of the `wrapper.java.initmemory` and `wrapper.java.maxmemory` parameters to the minimums given for the initial and maximum Java heap size, respectively, in "Tuning Settings" in the *NA Support Matrix*.

- If the values meet or exceed the recommendations, no action is required and you can stop here.
- If the values are lower than the recommendations, continue with step 6.

6 If necessary, set the `wrapper.java.initmemory` and `wrapper.java.maxmemory` parameters to the minimums given for the initial and maximum Java heap size, respectively, in "Tuning Settings" in the *NA Support Matrix*.

7 Set the young generation size as follows:

a To determine whether the young generation size has been set previously, search for the string `-Xmn`.

— If this string is in the file, edit this line to set the recommended value for the young generation size in "Tuning Settings" in the *NA Support Matrix*.

For example:

```
wrapper.java.additional.3=-Xmn2730m
```

— If this string is not in the file, add continue with step b.

b Search for the string `Additional` to locate the `Java Additional Parameters` section.

c After the last uncommented line in this section, add the following line:

```
wrapper.java.additional.N=-XmnYGm
```

d In the newly added line, make the following substitutions:

— Replace *N* with the next number in the sequence of uncommented `wrapper.java.additional` parameters.

For example, if the `wrapper.java.additional.11` parameter is uncommented and the `wrapper.java.additional.12` parameter is commented out with a number sign (`#`), set *N* to 12.

— Replace *YG* with the recommended value for the young generation size in "Tuning Settings" in the *NA Support Matrix*.

For example:

```
wrapper.java.additional.12=-Xmn2730m
```

8 Restart all NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  `/etc/init.d/truecontrol restart`

-

Configuring MySQL for NA

Restricting MySQL to a small number of concurrent threads can reduce NA performance. To avoid this problem, configure MySQL to use an infinite number of threads. This configuration varies across versions of MySQL. NA ships with MySQL 5.0.58, which interprets the value 20 for `innodb_thread_concurrency` as infinite.

For new installations of NA 9.20 or later, MySQL is configured with this setting.

For upgrades to NA from a version before 9.20, the recommended tuning is described in "Verify the MySQL Configuration" in the *NA Installation and Upgrade Guide*.

Configuring Oracle for NA

This section describes known tuning of Oracle for NA.

Number of Database Connections from NA

The number of database connections is the total number of connections that NA can make to the database at any moment. This number depends primarily on the NA configuration for the maximum number of concurrent tasks.

If you change the maximum data source pool size, update the Oracle database configuration for the number of database connections.

Additionally, the following errors indicate the need to update the configuration for the number of database connections:

- This task did not complete. Connections could not be acquired from the underlying database!
- This task did not complete. An SQLException was provoked by the following failure: com.mchange.v2.resourcepool.ResourcePoolException: A ResourcePool cannot acquire a new resource -- the factory or source appears to be down.
- This task did not complete. Can't find CustomScript
  Find failed: java.sql.SQLException: Connections could not be acquired from the underlying database!

For an Oracle database, the value of the `processes` parameter sets the number of database connections. The value of the `processes` parameter should be greater than or equal to the sum of the following factors:

- For *each* active NA core, the value of the maximum pool size attribute for the NA data source configuration
- For *each* active NA core, the value of the maximum pool size attribute for the NA report data source configuration
- For *each* active NA core, a buffer of 50

If the active NA cores in an NA Horizontal Scalability environment are configured identically, the calculation in this step is the same as multiplying the result of the calculation for one NA core by the number of active NA cores in the NA Horizontal Scalability environment.

According to the Oracle documentation, the values of the `sessions` and `transactions` parameters are relative to the value of the `processes` parameter. If the value of the `processes` parameter needs to be changed, the values of the `sessions` and `transactions` parameters should also be updated.

Size of the NA Tablespace

The following error suggests that the NA tablespace does not have sufficient space for its contents:

> The system could not save the data for device id 50851 - An SQLException was provoked by the following failure: com.mchange.v2.resourcepool.ResourcePoolException: A ResourcePool cannot acquire a new resource -- the factory or source appears to be down. Contact Technical Support. (Reference stack trace ID 1690)"

Report this message to the database administrator (DBA), and suggest that the DBA evaluate the free space of the NA tablespace.

Also see Reclaiming Unused Space (Oracle) on page 169.

Configuring SQL Server for NA

At this time, there is no recommended tuning for Microsoft SQL Server with NA.

6 Localization Concerns

This chapter describes known differences and configuration requirements for HP Network Automation Software (NA) running in a non-English language. It contains the following topics:

Summary Report Generation

The following error indicates that NA does not correctly interpret the date format of the NA server:

> The Generate Summary Reports tasks fail with : There was a problem generating the Summary Reports: javax.ejb.EJBException: RuntimeException

When this error occurs, the `jboss_wrapper.log` file contains the following error:

> Caused by: java.sql.SQLException: ORA-01843: invalid month

(The string invalid month is written in the localized language.)

In response to this error, configure NA with the date format that the NA server is using. Follow these steps:

1. Determine the system date format on the NA server.

   (On Windows operating systems, use the Short Date on the Formats tab of the Region and Language control panel.)

2. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *UNIX*: `<NA_HOME>/jre`
3. Back up the `reporting.rcx` file to a location outside the `<NA_HOME>` directory.
4. In a text editor such as WordPad or vi, open the `reporting.rcx` file.
5. Search for the string `TO_CHAR` to locate the following lines:

```
<value>
   select TO_CHAR(dal.CreateDate, 'MM/DD/YYYY'), count(*)
   from RN_DEVICE_ACCESS_LOG dal, RN_DEVICE dev
   where dal.DeviceID = dev.DeviceID
   and ActionTaken like 'New config id%'
   and (AccessTrigger is NULL or AccessTrigger not like '%user-modified%')
   and TO_DATE(SYSDATE, 'dd-mon-yyyy') - TO_DATE(dal.CreateDate,
'dd-mon-yyyy') &lt; 14
   group by TO_CHAR(dal.CreateDate, 'MM/DD/YYYY'),
```

```
TO_CHAR(dal.CreateDate,'DDD')
   order by TO_CHAR(dal.CreateDate,'DDD')
</value>
```

6 Within the identified lines, change each instance of the date format to match the system date format of the NA server. (Change two instances of `MM/DD/YYYY` and two instances of `dd-mon-yyyy`.)

For example, if the system date format is yyyy/MM/dd, update this section to read:

```
<value>
   select TO_CHAR(dal.CreateDate, 'YYYY/MM/DD'), count(*)
   from RN_DEVICE_ACCESS_LOG dal, RN_DEVICE dev
   where dal.DeviceID = dev.DeviceID
   and ActionTaken like 'New config id%'
   and (AccessTrigger is NULL or AccessTrigger not like '%user-modified%')
   and TO_DATE(SYSDATE, 'yyyy-mm-dd') - TO_DATE(dal.CreateDate,
'yyyy-mm-dd') &lt; 14
   group by TO_CHAR(dal.CreateDate, 'YYYY/MM/DD'),
TO_CHAR(dal.CreateDate,'DDD')
   order by TO_CHAR(dal.CreateDate,'DDD')
</value>
```

7 Reload the `.rcx` settings by doing *one* of the following:

- Run the `reload server options` command from the NA proxy.
- On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
- Restart the NA management engine.

Upgrading NA might overwrite the `reporting.rcx` file. Be prepared to replicate this configuration change after every upgrade.

Other Information

For more information about known differences when running NA in a non-English language, see the *NA Read Me* file, which is available

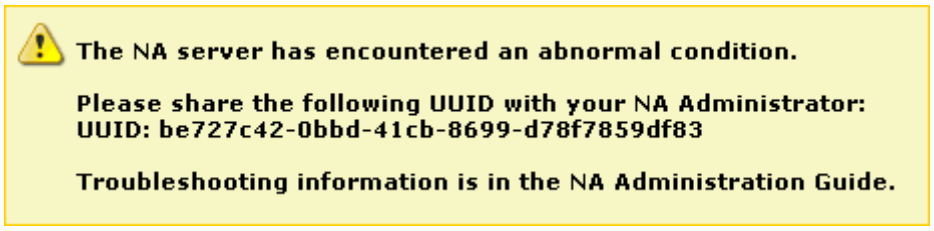
http://h20230.www2.hp.com/selfsolve/manuals

The *NA Read Me* file is not available in English.

7 Troubleshooting an Abnormal Condition on the NA Server

Occasionally, NA users might see a message similar to that shown in Figure 2.

Figure 2 Example Abnormal Condition Message



When such a condition occurs, NA logs a detailed message to the following file:

- *Windows*: `%NA_HOME%\server\log\jboss_wrapper.log`
- *UNIX*: `$NA_HOME/server/log/jboss_wrapper.log`

In the log file, a UUID identifies the message that describes this occurance of the abnormal condition. This UUID is included in the message presented to the NA console user. The user can copy the UUID from the message for pasting into communication with the NA administrator. In the example message shown in Figure 2, the UUID is `be727c42-0bbd-41cb-8699-d78f7859df83`.

For information about a specific condition, search the `jboss_wrapper.log` file for the UUID listed in the message. The relevant troubleshooting information is included in a block that begins with the following string:

```
========MSG BEGIN=============
```

The block ends with the following string:

```
=========MSG END============
```

8 Working with .rcx Files

The HP Network Automation Software (NA) property files use the `.rcx` extension. NA reads `.rcx` files in reverse alphabetical order. If a given setting is in multiple `.rcx` files, NA uses the last-read value. Thus, the settings in the `adjustable_options.rcx` file take precedence over the settings in the other `.rcx` files installed with NA.

At startup, NA reads *all* files in the `jre` directory and interprets their contents for NA configuration options. For this reason, save all backup copies of `.rcx` files outside the root NA directory.

In Horizontal Scalability environments, NA shares the actual values of most settings, not the `.rcx` files, across the NA cores. When a setting is modified on one NA core, that setting is replicated to the other NA cores. If an NA core is not operational during the change replication, that NA core does not receive the change. In that case, at a later time, use the Admin > Distributed > Renew Configuration Options page to push changes to other NA cores.

The distributed system options section of the `appserver.rcx` file lists the settings that are specific to one NA core and are not shared across the NA cores.

Some configuration changes require `.rcx` file modifications. The `.rcx` files are located in the following directory:

- *Windows*: `<NA_HOME>\jre\`
- *Unix*: `<NA_HOME>/jre/`

Always edit `.rcx` files with care. These files use XML format. If a `.rcx` file change results in invalid XML, the NA console might not start correctly.

It is recommended to make all configuration changes in the `adjustable_options.rcx` file. NA patch installations and product upgrades might overwrite any of the other NA-installed `.rcx` files.

The general procedure for changing `.rcx` files is as follows:

1. Back up the `.rcx` file to a location outside the `<NA_HOME>` directory.

   (NA reads all `.rcx` files within the NA directory structure.)
2. Add new content or update existing content as described in the instructions.
3. Save the `.rcx` file.

4 Reload the `.rcx` settings by doing *one* of the following:

- In the NA console, on the Admin > Administrative Settings > User Interface page, click **Save**.
- Run the `reload server options` command from the NA proxy.
- Restart the NA services.

Some changes do not take effect until the NA services have been restarted.

9 Configuring the NA Determination of Which User Changed a Device

As of HP Network Automation Software (NA) 9.20 Patch 1, the NA administrator can adjust the priorities that NA uses for associating a user to a specific device change. By default, NA uses the following priorities (1 is the highest priority):

1. User who scheduled a password change that was run on the device.
2. User who scheduled a software update that was run on the device.
3. User who deployed a configuration to the device.
4. User who ran a script on the device.
5. User who connected to the device through the system's proxy.
6. User information gathered from AAA logs.
7. User information parsed from a syslog message.
8. User who scheduled a diagnostic that was run on the device.

NA associates a weighted value to each priority. These weights can be adjusted using settings in the `adjustable_options.rcx` file.

To change the default order of these priorities, follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *UNIX*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In the `adjustable_options.rcx` file, add the following lines:

```
<option name="changepriority/ACL_DELETE_PRIORITY">21</option>
<option name="changepriority/PASSWORD_CHANGE_PRIORITY">20</option>
<option name="changepriority/SOFTWARE_UPDATE_PRIORITY">18</option>
<option name="changepriority/CONFIGURE_SYSLOG_PRIORITY">17</option>
<option name="changepriority/CONFIG_DEPLOY_PRIORITY">16</option>
<option name="changepriority/SCRIPT_RUN_PRIORITY">15</option>
<option name="changepriority/PROXY_PRIORITY">12</option>
<option name="changepriority/SYSLOG_PRIORITY">10</option>
<option name="changepriority/AAA_PRIORITY">8</option>
<option name="changepriority/DIAGNOSTIC_RUN_PRIORITY">2</option>
<option name="changepriority/NONE_PRIORITY">0</option>
```

4. As needed, change the value for each priority to reflect the desired priority order. The higher the value, the higher the priority.

   Each value must be an integer and unique within this list of priorities.

5. Save the `adjustable_options.rcx` file.

6 Reload the `.rcx` settings by doing *one* of the following:

- Run the `reload server options` command from the NA proxy.
- On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click **Save**.
- Restart the NA management engine.

To verify that the new values are being used, set Feature/ChangeDetection to trace.

10 Using Certificates with NA

A certificate provides proof of identification in any of the following exchanges:

- The web server identifies itself to the browser.
- One server identifies itself to another server.
- A user identifies themself to a web server.

This certificate can be self-signed or signed by a certificate authority (CA). HP Network Automation Software (NA) uses the following certificate files:

- The Truecontrol key store file stores private keys and certificates with their corresponding public keys. It is located as follows:
  - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf\truecontrol.keystore`
  - *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf/truecontrol.keystore`
- The Truecontrol trust store file contains certificates from other parties that you expect to communicate with, or from certificate authorities that you trust to identify other parties. It is located as follows:
  - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf\truecontrol.truststore`
  - *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf/truecontrol.truststore`

  The `truecontrol.truststore` file is new as of NA version 9.20.

- The CAcerts key store file also stores private keys and certificates with their corresponding public keys. The NA Java processes use the cacerts file when connecting to an SSL-based service (for example LDAP over SSL). It is part of the Java Development Kit (JDK) installed with NA and is located as follows:
  - *Windows*: `<NA_HOME>\jre\lib\security\cacerts`
  - *UNIX*: `<NA_HOME>/jre/lib/security/cacerts`

This chapter contains the following topics:

Default NA Certificates

At installation, NA includes self-signed certificates in the Truecontrol key store, Truecontrol trust store, and the CAcerts key store. The NA-provided certificates are the same on all NA servers. For that reason, it is recommended to replace the default self-signed certificates with a new self-signed or CA-signed certificate. For information, see Adding a Self-Signed Certificate to NA on page 94 or Adding a CA-Signed Certificate to NA on page 97.

Truecontrol Key Store

The `truecontrol.keystore` file contains the certificate that the web browser uses to identify the NA server. Table 16 lists the key properties of the NA-provided self-signed certificate. Property labels and value formats vary across web browsers.

Table 16 Properties of the Default Certificate for Accessing the NA Console

Property	Default Value
Issued to and by	localhost, Hewlett Packard Company • CN = localhost • OU = Hewlett Packard Company • O = Hewlett Packard Company • L = Palo Alto • S = CA • C = US
Serial number	48 4e 9d 84
Valid date range	June 10, 2008 to June 08, 2018
SHA1 fingerprint	05 de dc 68 58 45 ca ea 88 ff 16 05 e7 65 a9 5b 23 29 d7 65
MD5 fingerprint	65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8

By default, web browsers do not trust self-signed certificates. Therefore, NA console users see an unknown certificate warning before the NA console logon page appears.

Accepting the Truecontrol Certificate in a Web Browser

When the Truecontrol certificate is not in a web browser's list of trusted certificates, the web browser might display a warning message regarding the validity of the certificate. To resolve this issue, follow these steps:

1. Verify that the certificate values are as expected.

   For the default NA-provided certificate, the values should match the information described in Table 16, though the formatting and display order might be different.

2. Follow the web browser procedure for adding the verified certificate to the list of trusteed certificates.

Viewing the Truecontrol Key Store

To view the contents of the `truecontrol.keystore` file from the command line, follow these steps:

1. Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:
   - *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`
   - *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`
2. Examine the contents of the Truecontrol key store file by entering the following command:
   - *Windows*:
     `<NA_HOME>\jre\bin\keytool.exe -list -keystore truecontrol.keystore`
   - *UNIX*:
     `<NA_HOME>/jre/bin/keytool -list -keystore truecontrol.keystore`

   When prompted for the key store password, enter: **`sentinel`**

   The key store output is of the following form:

```
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
sentinel, 10-Jun-2008, PrivateKeyEntry,
Certificate fingerprint (MD5): 65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8
```

Alternatively, use the `-v` (verbose) option for more output in the following form:

```
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: sentinel
Creation date: 10-Jun-2008
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=localhost, OU=Hewlett Packard Company, O=Hewlett Packard Company, L=Palo Alto,
ST=CA, C=US
Issuer: CN=localhost, OU=Hewlett Packard Company, O=Hewlett Packard Company, L=Palo Alto,
ST=CA, C=US
Serial number: 484e9d84
Valid from: Tue Jun 10 16:28:04 BST 2008 until: Fri Jun 08 16:28:04 BST 2018
Certificate fingerprints:
         MD5:  65:94:D1:A0:44:84:E2:69:A4:23:DC:B9:5E:EB:91:A8
         SHA1: 05:DE:DC:68:58:45:CA:EA:88:FF:16:05:E7:65:A9:5B:23:29:D7:65
         Signature algorithm name: SHA1withRSA
         Version: 3
```

Truecontrol Trust Store

At NA installation, the `truecontrol.truststore` file contains one self-signed certificate. You can add other products' certificates to this file to support inter-application communication across secure sockets layer (SSL).

For information about importing the HP Network Node Manager i Software certificate into the `truecontrol.truststore` file, see the *HP Network Node Manager i Software–HP Network Automation Integration Guide*.

Adding a Self-Signed Certificate to NA

You can create a new self-signed certificate that is unique to your environment. Using a new self-signed certificate does not require third-party involvement but could require that each NA console user configure their web browser to trust the new self-signed certificate.

To create a self-signed certificate and add it to NA, follow these steps:

1 Generate a new self-signed certificate as follows:

a Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

— *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`

— *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`

b Create a backup copy of the `truecontrol.keystore` file.

c Use the `keytool` command to generate a new certificate in the Truecontrol key store file. For example:

— *Windows*:
```
<NA_HOME>\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \
-validity 3650 -alias nacert -keystore truecontrol.keystore
```

— *UNIX*:
```
<NA_HOME>/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \
-validity 3650 -alias nacert -keystore truecontrol.keystore
```

When prompted for the key store password, enter: **`sentinel`**

For more information, run the `keytool` command with no options.

d Enter the requested information:

— When prompted for your first and last name, enter the identifier of the NA server, which could be `localhost`, the short hostname, or the IP address.

Do *not* enter the fully-qualified domain name (FQDN) of the NA server.

Using a value other than `localhost` adds an additional configuration step that requires restarting the NA services.

— When prompted to confirm the organization informtion (for example, `Is CN=hostname, OU=someOU, O=someORG, L=someCITY, ST=someSTATE, C=AB correct? [no]:`), type **`yes`**, and then press **Enter**.

— When prompted for a password, press **Enter** to use the key store password.

2 Use the `keytool` command to export the newly-created certificate to a file. For example, from the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

- *Windows*:
```
<NA_HOME>\jre\bin\keytool.exe -export -alias nacert \
-file nacert.cer -keystore truecontrol.keystore
```
- *UNIX*:
```
<NA_HOME>/jre/bin/keytool -export -alias nacert -file nacert.cer \
-keystore truecontrol.keystore
```

When prompted for the key store password, enter: **sentinel**

Specify the alias used when generating the certificate in step 1 on page 94.

The output file (for example, nacert.cer) is created in the location from which the command is run.

The command output is of the following form:

```
Certificate stored in file nacert.cer
```

3 Import the exported certificate into the CAcerts key store as follows:

a Move the export file from its current location to the directory that contains the cacerts file. For example, from the directory that contains the truecontrol.keystore and truecontrol.truststore files:

— *Windows*: `move nacert.cer <NA_HOME>\jre\lib\security`

— *UNIX*: `mv nacert.cer <NA_HOME>/jre/lib/security`

b Change to the directory that contains the cacerts file:

— *Windows*: `<NA_HOME>\jre\lib\security`

— *UNIX*: `<NA_HOME>/jre/lib/security`

c Create a backup copy of the cacerts file.

d Use the keytool command to import the new certificate into the CAcerts key store file. For example:

— *Windows*:

```
<NA_HOME>\jre\bin\keytool.exe -import -alias nacert \
-file nacert.cer -keystore cacerts
```

— *UNIX*:

```
<NA_HOME>/jre/bin/keytool -import -alias nacert -file nacert.cer \
-keystore cacerts
```

When prompted for the key store password, enter: **changeit**

When prompted to trust the certificate, type **yes**, and then press **Enter**.

Specify the file (for example, nacert.cer) created in step 2 on page 94.

The alias is the identifier of the new certificate in the cacerts file. It does not need to match the alias in the truecontrol.keystore file.

The command output is of the following form:

```
Owner: CN=myhost, OU=Some OU, O=Some O, L=Mytown, ST=My State, C=AB
Issuer: CN=myhost, OU=Some OU, O=Some O, L=Mytown, ST=My State, C=AB
Serial number: 4e79d241
Valid from: Wed Sep 21 13:02:09 BST 2011 until: Sat Sep 18 13:02:09 BST 2021
Certificate fingerprints:
         MD5:  FA:B1:86:18:18:47:43:30:8B:38:38:E6:8E:73:DB:84
         SHA1: CC:F2:69:F3:2C:7E:8E:03:BE:EC:F2:18:78:80:41:0A:BA:95:48:F8
         Signature algorithm name: SHA1withRSA
         Version: 3
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

4 To force NA to use the new certificate, remove the NA-provided certificate from the Truecontrol key store as follows:

a Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

— *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`

— *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`

b Use the `keytool` command to export the sentinel certificate to a backup file. For example:

— *Windows*:
```
<NA_HOME>\jre\bin\keytool.exe -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

— *UNIX*:
```
<NA_HOME>/jre/bin/keytool -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

When prompted for the key store password, enter: **`sentinel`**

The command output is of the following form:

```
Certificate stored in file sentinel_from_truecontrol_keystore.cer
```

c Move the backup file (for example, `sentinel_from_truecontrol_keystore.cer`) to a safe location.

d Use the `keytool` command to delete the existing sentinel certificate from the Truecontrol key store. For example:

— *Windows*:
```
<NA_HOME>\jre\bin\keytool.exe -delete -alias sentinel \
-keystore truecontrol.keystore
```

— *UNIX*:
```
<NA_HOME>/jre/bin/keytool -delete -alias sentinel \
-keystore truecontrol.keystore
```

When prompted for the key store password, enter: **`sentinel`**

The command output is of the following form:

```
[Storing truecontrol.keystore]
```

5 *Optional*. In step 1 on page 94, if the identifier of the NA server was *not* `localhost`, update the NA configuration as follows:

a Change to the directory that contains the `.rcx` files:

— *Windows*: `<NA_HOME>\jre`

— *UNIX*: `<NA_HOME>/jre`

b Back up the `adjustable_options.rcx` file to a location outside of the `<NA_HOME>` directory.

c In the `adjustable_options.rcx` file, add the following line:

```
<option name="startup/precompile/http.prefix">http://"hostname"/</option>
```

d In the new line, replace `hostname` with the identifier entered for first and last name in step d of step 1 on page 94.

e Save the `adjustable_options.rcx` file.

Completing this step improves the NA console user experience by removing the wait time for each new page within the NA console.

6 Restart all NA services:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  ```
  /etc/init.d/truecontrol restart
  ```

7 Instruct each NA console user to add the new certificate to their web browser's list of trusted certificates.

Adding a CA-Signed Certificate to NA

Using a new CA-signed certificate requires interaction with a third-party but does not require that each NA console user configure their web browser to trust the certificate.

To request a CA-signed certificate and add it to NA, follow these steps:

1 Generate a new local certificate as follows:

a Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

- *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`
- *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`

b Create a backup copy of the `truecontrol.keystore` file.

c Use the `keytool` command to generate a new certificate in the Truecontrol key store file. For example:

- *Windows*:
  ```
  <NA_HOME>\jre\bin\keytool.exe -genkey -keyalg RSA -keysize 2048 \
  -validity 3650 -alias nacacert -keystore truecontrol.keystore
  ```
- *UNIX*:
  ```
  <NA_HOME>/jre/bin/keytool -genkey -keyalg RSA -keysize 2048 \
  -validity 3650 -alias nacacert -keystore truecontrol.keystore
  ```

When prompted for the key store password, enter: **`sentinel`**

Note the alias used for generating the new certificate. You must use this same alias for generating the certificate signing request in step 2 on page 98 and for importing the generated certificates into the `truecontrol.keystore` and `truecontrol.truststore` files in step 4, step d on page 99.

For more information, run the `keytool` command with no options.

d Enter the requested information:

— When prompted for your first and last name, enter the fully-qualified domain name (FQDN) of the NA server.

— When prompted to confirm the organization informtion (for example, `Is CN=hostname, OU=someOU, O=someORG, L=someCITY, ST=someSTATE, C=AB correct? [no]:`), type **`yes`**, and then press **Enter**.

— When prompted for a password, press **Enter** to use the key store password.

2 Use the `keytool` command to create a certificate signing request (CSR) from the new local certificate. For example, from the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

- *Windows*:
```
<NA_HOME>\jre\bin\keytool.exe -certreq -alias nacacert \
-file narequest.csr -keystore truecontrol.keystore
```
- *UNIX*:
```
<NA_HOME>/jre/bin/keytool -certreq -alias nacacert -file narequest.csr
\
-keystore truecontrol.keystore
```

Specify the alias used when generating the local certificate in step 1 on page 97.

The output file (for example, `narequest.csr`) is created in the location from which the command is run.

3 Submit the CSR to the CA. If given the option, request that the new certificate be in a Tomcat-compatible or Apache-compatible format.

The CA should return one of the following:

- One file, a signed certificate, referred to as `server.crt` in this procedure.

  The `server.crt` file contains both the server certificate (the top certificate contained in the file) and one or more CA certificates (the last certificates contained in the file).

  In a text editor such as WordPad or vi, copy the contents of the CA certificate into a new file, the `CA.crt` file.

  Use the `server.crt` file when importing the server certificate into the `truecontrol.keystore` file and the `CA.crt` file when importing the CA certificate into the `truecontrol.truststore` file.

- Two files, referred to as `server.crt` and `CA.crt` in this procedure.

  In a text editor such as WordPad or vi, add the contents of the `CA.crt` file to the end of the `server.crt` file.

  Use the modified `server.crt` file when importing the server certificate into the `truecontrol.keystore` file and the `CA.crt` file when importing the CA certificate into the `truecontrol.truststore` file.

The following examples show what the CA-provided files might look like:

Combined server and CA certificates in one file:

```
-----BEGIN CERTIFICATE-----
Sample1/VQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.....................................................................
.....................................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Sample2/Gh0dHA6Ly9jb3JwMWRjc2cyLnNnLmludC5wc2FnbG9iYWwuY29tL0Nlc
RaOCApwwggKYMB0GA1UdDgQWBBSqaWZzCRcpvJWOFPZ/Be9b+QSPyDAfBgNVHSMC
.....................................................................
.....................................................................
Wp5Lz1ZJAOu1VHbPVdQnXnlBkx7V65niLoaT90Eqd6laliVlJHj7GBriJ90uvVGu
BQagggEChoG9bGRhcDovLy9DTj1jb3JwMWRjc2cyL==
-----END CERTIFICATE-----
```

Separate server and CA certificate files:

```
-----BEGIN CERTIFICATE-----
Sample/AVQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.....................................................................
.....................................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
```

4 Import the (modified if necessary) `server.crt` file into the Truecontrol key store and the `CA.crt` file into the Truecontrol trust store as follows:

   a Copy the `server.crt` and `CA.crt` files to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

      — *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`

      — *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`

   b Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

      — *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`

      — *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`

   c Create backup copies of the `truecontrol.keystore` and `truecontrol.truststore` files.

   d Use the `keytool` command to import the new certificates into the correct files. (One command for each certificate.) For example:

      — *Windows*:

```
<NA_HOME>\jre\bin\keytool.exe -import -trustcacerts \
-alias nacacert -file server.crt -keystore truecontrol.keystore

<NA_HOME>\jre\bin\keytool.exe -import -trustcacerts \
-alias nacacert -file CA.crt -keystore truecontrol.truststore
```

— *UNIX*:

```
<NA_HOME>/jre/bin/keytool -import -trustcacerts -alias nacacert \
-file server.crt -keystore truecontrol.keystore

<NA_HOME>/jre/bin/keytool -import -trustcacerts -alias nacacert \
-file CA.crt -keystore truecontrol.truststore
```

When prompted for the key store password, enter: **`sentinel`**

When prompted to trust the certificate, type **`yes`**, and then press **Enter**.

The alias is the identifier of the new certificate in each file. It must match the alias used to generate the certificate signing request in step 2 on page 98.

The command output is of the following form:

```
Owner: CN=NA_server.example.com
Issuer: CN=NA_server.example.com
Serial number: 4e79d241
Valid from: Wed Sep 21 13:02:09 BST 2011 until: Sat Sep 18 13:02:09 BST 2021
Certificate fingerprints:
         MD5:  FA:B1:86:18:18:47:43:30:8B:38:38:E6:8E:73:DB:84
         SHA1: CC:F2:69:F3:2C:7E:8E:03:BE:EC:F2:18:78:80:41:0A:BA:95:48:F8
         Signature algorithm name: SHA1withRSA
         Version: 3
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

e. Repeat step d until all CA-provided certificates have been imported into the `truecontrol.keystore` file.

5. To force NA to use the new certificate, remove the NA-provided certificate from the Truecontrol key store as follows:

a. Change to the directory that contains the `truecontrol.keystore` and `truecontrol.truststore` files:

— *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`

— *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`

b. Use the `keytool` command to export the sentinel certificate to a backup file. For example:

— *Windows*:

```
<NA_HOME>\jre\bin\keytool.exe -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

— *UNIX*:

```
<NA_HOME>/jre/bin/keytool -export -alias sentinel \
-file sentinel_from_truecontrol_keystore.cer \
-keystore truecontrol.keystore
```

When prompted for the key store password, enter: **`sentinel`**

The command output is of the following form:

```
Certificate stored in file sentinel_from_truecontrol_keystore.cer
```

c. Move the backup file (for example, `sentinel_from_truecontrol_keystore.cer`) to a safe location.

d Use the `keytool` command to delete the existing sentinel certificate from the Truecontrol key store. For example:

— *Windows*:
```
<NA_HOME>\jre\bin\keytool.exe -delete -alias sentinel \
-keystore truecontrol.keystore
```

— *UNIX*:
```
<NA_HOME>/jre/bin/keytool -delete -alias sentinel \
-keystore truecontrol.keystore
```

When prompted for the key store password, enter: **`sentinel`**

The command output is of the following form:

```
[Storing truecontrol.keystore]
```

6 Update the NA configuration as follows:

a Change to the directory that contains the `.rcx` files:

— *Windows*: `<NA_HOME>\jre`

— *UNIX*: `<NA_HOME>/jre`

b Back up the `adjustable_options.rcx` file to a location outside of the `<NA_HOME>` directory.

c In the `adjustable_options.rcx` file, add the following line:

```
<option name="startup/precompile/http.prefix">http://"hostname"/</option>
```

d In the new line, replace `hostname` with the identifier entered for first and last name in step d of step 1 on page 97.

e Save the `adjustable_options.rcx` file.

Completing this step improves the NA console user experience by removing the wait time for each new page within the NA console.

7 Restart all NA services:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  `/etc/init.d/truecontrol restart`

8 Test the new certificate by logging on to the NA console. If the web browser trusts the CA, it will trust the connection to the NA console with no warning message.

Adding a CA Root Certificate to NA

One step in enabling Public Key Infrastructure (PKI) user authentication is to import a copy of the certificate authority (CA) root certificate into the Truecontrol trust store. Completion of this step ensures that NA trusts the issuer of the certificates that users present while logging on to NA.

Import one copy of the root certficate for each CA that generates user certificates.

To import the CA root certificate into NA, follow these steps:

1. Obtain the root certificate from the CA.

   This procedure identifes the root certificate as `root.crt`.

2. Import the `root.crt` file into the Truecontrol trust store as follows:

   a. Copy the `root.crt` file to the directory that contains the `truecontrol.truststore` file:

      — *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`

      — *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`

   b. Change to the directory that contains the `truecontrol.truststore` file:

      — *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`

      — *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`

   c. Create a backup copy of the `truecontrol.truststore` file.

   d. Use the `keytool` command to import the root certificate into the Truecontrol trust store file. For example:

      — *Windows*:
      ```
      <NA_HOME>\jre\bin\keytool.exe -import -trustcacerts \
      -alias rootcert -file root.crt -keystore truecontrol.truststore
      ```

      — *UNIX*:
      ```
      <NA_HOME>/jre/bin/keytool -import -trustcacerts -alias rootcert \
      -file root.crt -keystore truecontrol.truststore
      ```

      When prompted for the trust store password, enter: **`sentinel`**

      For more information, run the `keytool` command with no options.

      When prompted to trust the certificate, type **`yes`**, and then press **Enter**.

      The alias is the identifier of the certificate in each file. The CA must provide the alias used in its root certificate.

      The command output is of the following form:

```
Owner: CN=Issuer.FTC.PKI Root CA, DC=ftcpki, DC=com
Issuer: CN=Issuer.FTC.PKI Root CA, DC=ftcpki, DC=com
Serial number: 6a265b0a1f77939d49c0055415511857
Valid from: Sat Feb 23 09:20:01 MST 2013 until: Mon Feb 23 09:30:00 MST 2043
Certificate fingerprints:
         MD5:  6A:35:83:40:67:76:9C:D7:21:4E:C4:D4:CC:4B:6E:15
         SHA1: 93:08:EB:27:77:79:23:F9:6D:9A:B9:5E:8F:DB:EF:91:6C:6E:9C:D8
         Signature algorithm name: SHA1withRSA
         Version: 3
```

```
Extensions:

#1: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 41 A9 C7 28 B3 36 11 18   F8 91 4D 58 51 8F 97 16  A..(.6....MXQ...
0010: E8 5C 03 E1                                        .\..
]
]

#4: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false

#5: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false

#6: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [1.2.3.4.1455.67.89.5]
[PolicyQualifierInfo: [
  qualifierID: 1.3.6.1.5.5.7.2.2
  qualifier: 0000: 30 2E 1E 2C 00 4C 00 65   00 67 00 61 00 6C 00 20  0..,.L.e.g.a.l.
0010: 00 50 00 6F 00 6C 00 69   00 63 00 79 00 20 00 53  .P.o.l.i.c.y. .S
0020: 00 74 00 61 00 74 00 65   00 6D 00 65 00 6E 00 74  .t.a.t.e.m.e.n.t

], PolicyQualifierInfo: [
  qualifierID: 1.3.6.1.5.5.7.2.1
  qualifier: 0000: 16 1F 68 74 74 70 3A 2F   2F 70 6B 69 2E 66 61 62  ..http://pki.fab
0010: 72 69 6B 61 6D 2E 63 6F   6D 2F 63 70 73 2E 74 78  rikam.com/cps.tx
0020: 74                                                 t

]]  ]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

3 Restart the NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  `/etc/init.d/truecontrol restart`
-

Troubleshooting

This section contains information about errors you might see while working with certificates in NA.

Incorrect Magic

Some operating systems, such as RedHat Linux, include a `keytool` utility. If the version of the keytool provided with the operating system does not match the NA JRE version, you will see an error message similar to the following:

```
keytool error: gnu.javax.crypto.keyring.MalformedKeyringException:
incorrect magic
```

In this case, use the keytool utility provided with NA:

- *Windows*: `<NA_HOME>\jre\bin\keytool.exe`
- *UNIX*: `<NA_HOME>/jre/bin/keytool`

httpmonitor Errors

If you change the certificate and do not import it into the CAcerts key store, you will see `httpmonitor` errors.

Correct this problem by importing the new certificate into the NA key store as described in Adding a Self-Signed Certificate to NA on page 94.

11 Enabling FIPS Mode

The Federal Information Processing Standardization (FIPS) specifies cryptography requirements for both software and hardware. FIPS applies to SSH connections to and from NA. When enabled, the default FIPS configuration applies to both of the following:

- SSH connections to the NA core
- SSH connections from the NA core to devices

For NA managed devices, FIPS functionality is only pertinent for SSH/SCP device access or SNMPv3 use. Devices that do not support SSH/SCP or SNMPv3 are not affected.

Enabling FIPS mode affects device access as follows:

- Restricts the encryption algorithms that can be used. For example, AES and 3DES are permitted; however Blowfish and DES are not.

  Because of this restriction, NA might not be able to communicate with non-FIPS compliant devices. In this case, do one of the following:

  — Configure NA to use a protocol other than SSH or SCP for connecting to non-FIPS compliant devices.

  — Disable FIPS for connections to all devices as described in the procedure for enabling FIPS.

- Replaces implementation of other encryption algorithms with a FIPS-compliant encryption algorithm.

To enable FIPS mode, follow these steps:

1 Add the following line to the `adjustable_options.rcx` file:

```
<option name="crypto/fips/enabled">true</option>
```

2 *Optional*. Configure the permitted encryption algorithms.

a Copy the following lines from the `appserver.rcx` file to the `adjustable_options.rcx` file:

```
<array name="crypto/fips/cipher_list">
   <value>3des-cbc</value>
   <value>aes128-cbc</value>
   <value>aes128-ctr</value>
   <value>aes192-cbc</value>
   <value>aes192-ctr</value>
   <value>aes256-cbc</value>
   <value>aes256-ctr</value>
</array>
```

```
<array name="crypto/fips/mac_list">
   <value>hmac-sha1</value>
   <value>hmac-sha1-96</value>
</array>
```

b For each encryption algorithm to block, delete the associated line in the `adjustable_options.rcx` file.

3 *Optional*. Disable FIPS for connections to all devices by adding the following line to the `adjustable_options.rcx` file:

```
<option name="crypto/fips/disabled_for_device_access">true</option>
```

4 Restart the NA management engine.

In the log file, a message incidates that FIPS mode is enabled. For example:

```
{system/crypto} [main] 75 FIPS140Mode: Loading FIPS JCE Provider
```

5 Log on to the NA console as an administrative user.

6 Open the View Details page (**Admin > System Status > BaseServerMonitor > View Details**).

In the text, the following line indicates that FIPS mode is enabled.

```
crypto/fips/enabled = true
```

To disable FIPS mode, follow these steps:

1 Add the following line to the `adjustable_options.rcx` file:

```
<option name="crypto/fips/enabled">false</option>
```

2 Restart the NA management engine.

12 Configuring NA to Support PKI User Authentication

As of NA 9.22, NA can authenticate a user based on the information in an X.509 format certificate. The certificate can be installed into the browser that runs the NA console. Alternatively, the certificate can be on a separate device, such as a smart card, that the user connects to the computer before opening the NA console. Public Key Infrastructure (PKI) user authentication enables both Common Access Card (CAC) and Personal Identity Verification (PIV) for user authentication into NA.

Enabling PKI user authentication impacts all users on all NA cores. Ensure that all NA users have X.509-format certificates or use an alternate user authentication method.

Enabling PKI user authentication does not impact device authentication.

While PKI user authentication is enabled, NA proxy sessions initiated from the NA console also use PKI user authentication. The NA API and NA proxy sessions initiated outside the NA console (for example, through telnet or SSH) do not support PKI user authentication.

This chapter contains the following topics:

For information about how NA determines whether to grant access to a PKI certificate user, see “User Authentication” in the *NA User Guide*.

Configure NA for PKI User Authentication

To configure NA to use X.509 format certificate authentication for accessing the NA console and the NA proxy from the NA console, follow these steps:

1. Import the certificate authority root certificate into the NA trust store as described in Adding a CA Root Certificate to NA on page 102.

   In a Horizontal Scalability or Multimaster Distributed System environment, import the certificate authority root certificate into the NA trust store on each NA core.

2. After restarting the NA services, log on to the NA console as a user with administrator privileges.

3 Configure NA user names and privileges.

NA consults a user directory to determine each user's access privileges. Each NA user name must match the certificate subject according to the mapping rules set on the Administrative Settings – User Authentication page of the NA console. For information about available mapping options, see "User Authentication" in the *NA User Guide*.

When the certificate subject includes the at sign (@), replace this character with the underscore character (_) in the NA user name.

- To use the NA database as the user directory, create and configure each NA user from the All Users page (**Admin** > **Users**) in the NA console.

With PKI user authentication, the process of connecting to the NA console validates that the password for the NA user in the NA database meets the security policies and has not expired. Additionally NA user passwords might be used for device authentication.

- To use a directory service as the user directory, use the LDAP Set-up Wizard as described in "LDAP External Authentication Setup" in the *NA User Guide*.

4 Verify that at least one of the NA users configured in step 3 belongs to the Administrator group.

While PKI user authentication is enabled, if the user name of the administrator user account created during NA installation does not correspond to a certificate, that account is not available for connecting to the NA console.

5 In the PKI Authentication section of the Administrative Settings – User Authentication page (**Admin** > **Administrative Settings** > **User Authentication**), specify the following:

- The location of the NA user directory
- The certificate fields that contain the NA user name (see Distinguished Names Example on page 109)
- The distinguished names of the trusted certificate issuers
- The certificate revocation checking configuration

For more information about these fields, see "User Authentication" in the *NA User Guide*.

6 In the External Authentication Type section of the Administrative Settings – User Authentication page, select **PKI**.

7 Click **Save**.

Configure NA for Smart Card Authentication

To configure NA to use smart card authentication for accessing the NA console and the NA proxy from the NA console, follow the steps in Configure NA for PKI User Authentication on page 107. In the PKI Authentication section of the Administrative Settings – User Authentication page (**Admin** > **Administrative Settings** > **User Authentication**), for the Extended Key Usage field, enter **`1.3.6.1.4.1.311.20.2.2`** (for smart card certificates).

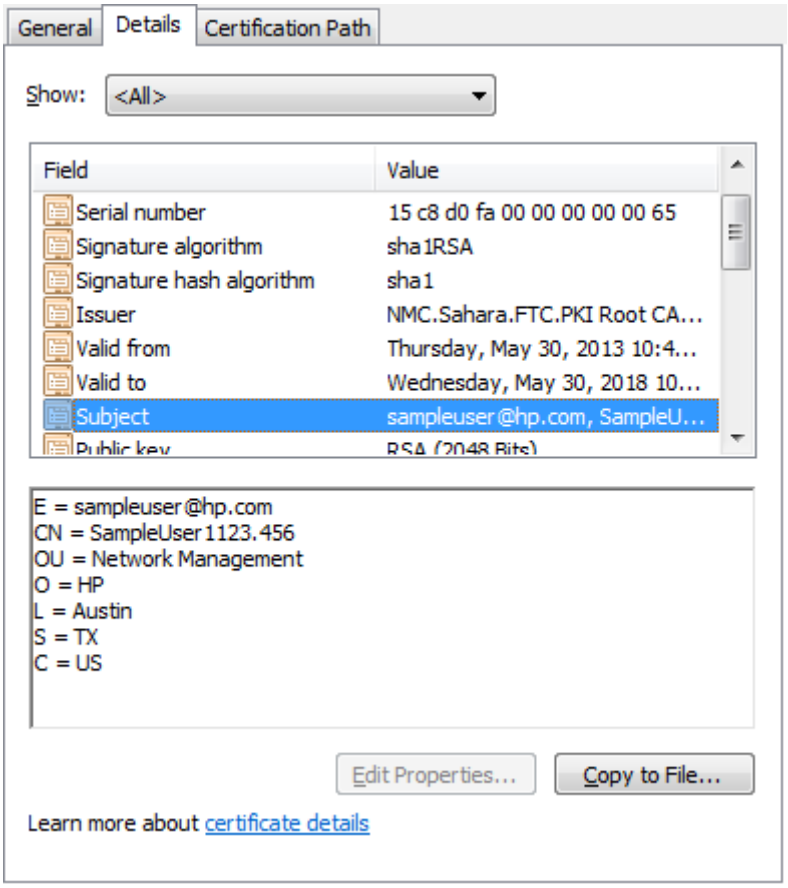
Distinguished Names Example

This section contains the following examples:

Certificate Subject

Figure 3 shows the Subject field of an X.509 format certificate. This Subject field contains the distinguished name of the certificate owner.

Figure 3 Subject Example



In this example, the elements of the distinguished name are as follows:

- Email address (`sampleuser@hp.com`)
- Common name (`SampleUser1123.456`)
- Organizational unit (`Network Management`)
- Organization (`HP`)
- Location (`Austin`)
- State (`TX`)
- Country (`US`)

To use the entire email address as the NA user name, enter `EMAILADDRESS` in the **Ordered Subject Attribute** field on the Administrative Settings – User Authentication page. In this case, create the NA user name as `sampleuser_hp.com` because NA does not support the use of the at sign (@) in user names.

To use a portion of the email address as the NA user name, enter `EMAILADDRESS=<regular_expression>` in the **Ordered Subject Attribute** field on the Administrative Settings – User Authentication page. Craft the regular expression to extract the NA user name from the email address.

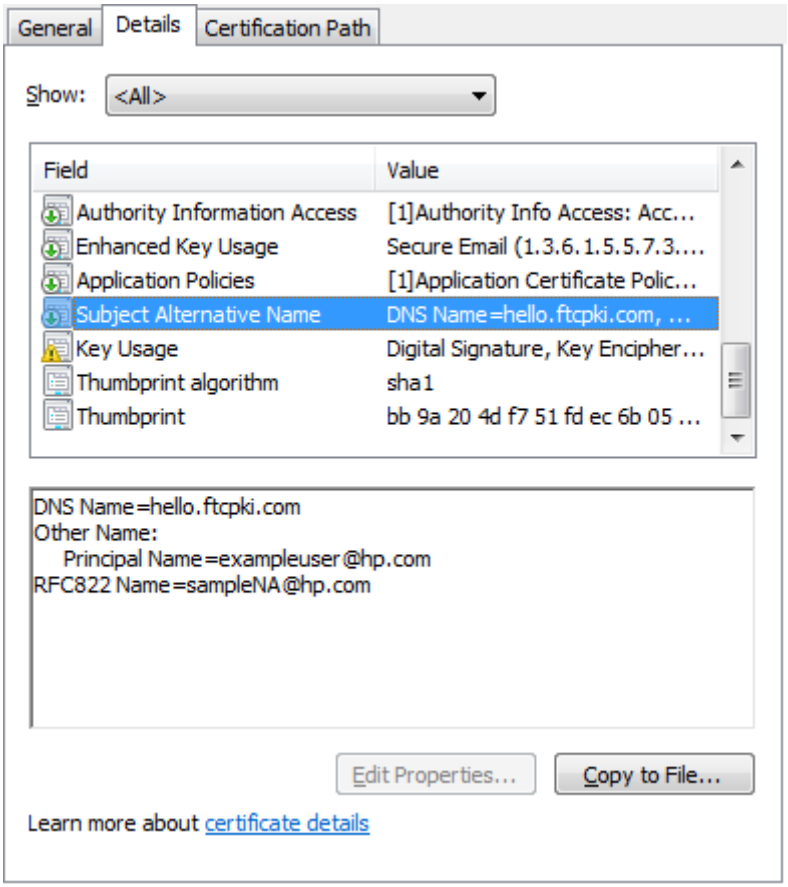
To use the common name as the NA user name, enter `COMMONNAME` in the Ordered Subject Attribute field on the Administrative Settings – User Authentication page.

NA does not support spaces in the user name. Therefore, the common name value cannot contain spaces when used as the NA user name.

Certificate Subject Alternative Name

Figure 4 shows the Subject Alternative Name field of an X.509 format certificate. This Subject Alternative Name field contains alternate identifiers of the certificate owner.

Figure 4 Subject Alternative Name Example



In this example, the elements of the subject alternative name that NA can process are as follows:

- Other Name with Principal Name value of `exampleuser@hp.com`
- RFC822 Name with value `sampleNA@hp.com`

For Other Name, NA supports the Principal Name (object identifier 1.3.6.1.4.1.311.20.2.3) only. The value of the Principal Name can be any kind of string, but the entire Principal Name value must match the NA user name.

To use the Principal Name value as the NA user name, enter **`otherName`** in the **Ordered Subject Alternative Name Types** field on the Administrative Settings – User Authentication page. Then, in the **Subject Alternative Name OID** field, enter **`1.3.6.1.4.1.311.20.2.3`**. In this case, create the NA user name as `exampleuser_hp.com` because NA does not support the use of the at sign (@) in user names.

To use the RFC822 Name as the NA user name, enter **`rfc822Name`** in the **Ordered Subject Alternative Name Types** field on the Administrative Settings – User Authentication page. In this case, create the NA user name as `sampleNA_hp.com` because NA does not support the use of the at sign (@) in user names.

Clear Authentication Data in the Browser

If the browser stores PKI certificate authentication data, logging out from NA is not sufficient to prevent unauthorized access to the NA console. Anyone who clicks **Log In** gains access to the NA console without further authorization. In this case, instruct all NA console users to close all browser windows after logging out from NA. Alternatively, users can clear all PKI certificate authentication data.

Clearing PKI certificate authentication data from the browser impacts all applications that used certificate-based user authentication to run in the browser.

To clear PKI certificate authentication data in Microsoft Internet Explorer, in the Internet Options dialog box, select the **Content** tab, and then click **Clear SSL State**.

To clear PKI certificate authentication data in Mozilla Firefox, do one of the following:

- On the menu bar, click **Tools**, then click **Clear Recent History**. In the Clear Recent History window, select **Active Logins** from the Details list, and then click **Clear Now**.
- Press **Ctrl**+**Shift**+**Delete**. In the Clear Recent History window, select **Active Logins** from the Details list, and then click **Clear Now**.

Disable PKI User Authentication

If you have access to the NA console, disable PKI user authentication by following these steps:

1. Log on to the NA console as a user with administrator privileges.
2. On the Administrative Settings – User Authentication page (**Admin** > **Administrative Settings** > **User Authentication**), set External Authentication Type to anything other than **PKI**.
3. Click **Save**.

If you do not have access to the NA console, disable PKI user authentication by following these steps:

This procedure requires editing configuration files that are crucial to NA functionality. Only follow these steps if you do not have access to the NA console. Verify all changes before saving the configuration files.

1 Stop the NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  `/etc/init.d/truecontrol stop`

2 Disable PKI user authentication in the PKI configuration file.

a Change to the directory that contains the configuration file:

- *Windows*: `<NA_HOME>\server\ext\jboss\server\default\conf`
- *UNIX*: `<NA_HOME>/server/ext/jboss/server/default/conf`

b Back up the `nms-auth-config.xml` file to a location outside the `<NA_HOME>` directory.

c In the `nms-auth-config.xml` file, locate the following lines:

```
<realms>
  <!-- valid modes are X509, BASIC or FORM. Not all realms support
  all modes. -->
  <realm name="console">
    <mode>X509</mode>
  </realm>
</realms>
```

d Change the mode line to read:

```
<mode>FORM</mode>
```

3 Disable PKI user authentication at the NA console level.

a Change to the directory that contains the `.rcx` files:

- *Windows*: `<NA_HOME>\jre`
- *UNIX*: `<NA_HOME>/jre`

b Back up the `site_options.xml` file to a location outside the `<NA_HOME>` directory.

c In the `site_options.xml` file, locate the following lines:

```
<option name="authentication/external/type">
  <title>External Authentication Type</title>
  …
  <comment>Choose the type of external authentication you would like
  to use. &lt;br&gt;
   If you choose TACACS+, RADIUS, HP Server Automation Software, or
```

```
PKI, configure that type in the related section on this page.
&lt;br&gt;SecurID has no additional external authentication
options. &lt;br&gt;
</comment>certificate</option>
```

d Change the option type from certificate to local:

```
</comment>local</option>
```

Be sure that you are working in the `<option name="authentication/external/type">` block.

4 Start the NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  `/etc/init.d/truecontrol start`

Users should now be able to log on to the NA console with the user name and password configured on the All Users (**Admin** > **Users**) page in the NA console.

13 Starting an External Application as a Non-Root User (Linux and Solaris only)

As of NA 9.22.01, you can configure NA to start the script named in the Run External Application task as a specific operating system user. Enabling this change removes the requirement for the root user to run the external scripts.

This topic applies to Linux and Solaris operating systems only.

To enable this feature, follow these steps:

1. Create or verify an operating system user account with read/write access to `/tmp`.

   By default, `/tmp` is the directory in which NA stores temporary scripts. If the `java.io.tmpdir` setting in the `<HA_HOME>/server/ext/wrapper/conf/jboss_wrapper.conf` file specifies a different location, ensure that the user account has access to that location.

2. Verify that the user account has access to the NA Expect directory and files and libraries:

   - `<NA_HOME>/server/ext/expect/*`
   - `<NA_HOME>/server/ext/wrapper/lib/libexpect5.39.so.1`

   If necessary, update ownership of these files, for example:

   ```
   chmod -R 755 <NA_HOME>/server/ext/wrapper/lib/libexpect5.39.so.1
   ```

3. Configure the user account's profile to set the NA environment variable `LD_LIBRARY_PATH` that points to the Expect libraries by editing the user's `.profile` file or `.bash_profile` file (depending on the operating system) to include the following lines:

   ```
   LD_LIBRARY_PATH=<NA_HOME>/server/ext/wrapper/lib:/usr/lib:/lib:/usr/local/lib
   export LD_LIBRARY_PATH
   ```

   Replace `<NA_HOME>` with the actual path of the NA home directory.

4. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.

5. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="scripting/os_user">OSUserName</option>
   ```

   Replace `OSUserName` with the name of a valid UNIX or Linux user account.

6. If the `su` command is not in the `/bin` directory on the NA core server, in the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="scripting/scripting/su_path">Path_TO_SU</option>
   ```

   Replace `Path_TO_SU` with the path to the directory that contains the `su` command.

7. Save the `adjustable_options.rcx` file.

8. Restart the NA services on all cores in the NA environment.

9 To run the scripts containing operating system commands from the Run External Application task, ensure that the operating system user account has permission to access and run the task.

14 Configuring NA to Permit Editing of Tasks Waiting for Approval

This topic applies only when NA is configured with workflow approval rules.

As of NA 9.22.01, tasks in the REQUESTED state can be viewed but cannot be edited.

To permit editing of tasks waiting for approval, follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="workflow/disable_task_edit">false</option>
   ```
4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing one of the following:
   - Run the reload server options command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click Save.
   - Restart the NA management engine.

15 Configuring the Task Completion Email Content

For each task, you can set NA to send an email message upon task completion. A group task is one that works on multiple devices. The devices on which a group task runs can be identified individually, through device groups, or by a combination of both approaches. As of NA 9.22, for a group task NA sends only one email message upon completion of the group task. Prior to NA 9.22, NA sent one email message upon completion of each child task.

Enabled event rules might send email messages regarding child task completion. To prevent these additional email messages, disable these event rules.

The format of the email content (subject and body) is the same for all tasks types but depends on whether the task is for one device or is a group task.

Single Task Completion Email Message Format

For a non-device task or a task that works on only one device, the default email message recipient is the task originator. This default is configurable.

For a non-device task or a task that works on only one device, the default format of the email message subject is as follows:

```
Task $TaskName$ completed. Task status: $TaskStatus$
```

For a non-device task or a task that works on only one device, the default format of the email message body is as follows:

```
Task          : $TaskName$
originated by : $OriginatorName$
scheduled on  : $TaskScheduleDate$
completed with the following status:
                $TaskStatus$.
The following devices have been processed:
                $TaskDevices$.
Task comments : $TaskComments$
View the task information here:
                $AppURL$/task.view.htm?taskID=$TaskID$
```

The default format produces an email message similar to the example shown in Table 17.

Table 17 Example of the Default Task Completion Email Message for a Single Task

Content Type	Example
Subject	Task Run Diagnostics completed. Task status: Succeeded
Body	Task : Run Diagnostics originated by : admin scheduled on : 2013-05-18 03:53:04.0 completed with the following status: Succeeded. The following devices have been processed: cisco_c3560 (10.78.60.36) Task comments : View the task information here: https://server.example.com:8443//task.view.htm?taskID=2801

Alternatively, the email message body can contain details of the task results. Enabling the task results option overrides the message body. Table 18 shows an example email message with task results.

Table 18 Example Email Message with Task Results

Content Type	Example
Subject	Task Run Diagnostics completed. Task status: Succeeded
Body	Task Name: Run Diagnostics Task ID: 192511 Status: Succeeded Comments: Added by: admin (chris admin) Task Priority: 3 Create Date: 2013-05-18 04:29:19.0 Device: cisco_c3560 (10.78.60.36) Schedule Date: As Soon As Possible Start Date: As Soon As Possible Complete Date: Sat May 18 04:29:19 MDT 2013 Duration: 1 Repeat type: Non-recurring View Task Details (may not be available if the records were pruned) Result Details: Diagnostic 'Hardware Information for Cisco IOS enable' completed. Policy check has failed. View Policy Events **Connect** - Succeeded Connected via telnet to 10.78.60.36 [in realm Default Realm] **Login / Authentication** - Succeeded Successfully used: Last successful password (Password rule Manager) View Hardware Information

To change the any of the format, contents, language, or default recipient of the email content for a single task, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In the `appserver.rcx` file, locate the following comment line:

   ```
   <!-- task email notification options -->
   ```

3. Copy the following blocks from the `appserver.rcx` file to the `adjustable_options.rcx` file:
   - `<option name="task/email/subject">...</option>`
   - `<option name="task/email/text">...</option>`
   - `<option name="task/email/includeResultDetails">false</option>`
4. Edit the subject and text values. Table 19 lists the available variables for use in these options.

5 To enable the inclusion of detailed task results in the message, set the `task/email/includeResultDetails` option to `true`:

```
<option name="task/email/includeResultDetails">true</option>
```

6 To change the default email message recipient, do the following:

a In the `adjustable_options.rcx` file, add the following line:

```
<option name="task/email/recipient"></option>
```

b Insert a comma-separated list of email address recipients.

To remove the default email message recipient, do not enter any email addresses. In this case, if the NA user who schedules the task neglects to enter an email address, the resulting message cannot be delivered.

7 Save the `adjustable_options.rcx` file.

8 Restart the NA services on all cores in the NA environment.

Table 19 Variables for the Task Completion Email Content

Variable	Description
$ApprovalDate$	Task approval date.
$ApproverEmails$	Comma separated list of email addresses of the task approvers.
$ApprovalPriority$	Task approval priority.
$OriginatorEmail$	The email address of the task originator.
$OriginatorFirstName$	The first name of the task originator.
$OriginatorLastName$	The last name of the task originator.
$OriginatorName$	The name of the task originator.
$TaskName$	The task name.
$TaskComments$	The task comments.
$TaskDevices$	A list of devices affected by the task.
$TaskFrequency$	The frequency of the task.
$TaskID$	The task identifier.
$TaskScheduleDate$	The task scheduled timestamp.
$TaskStatus$	The task status. For example; Succeeded, Failed, or Skipped.

Group Task Completion Email Message Format

For a task that works on multiple devices, the default email message recipient is the task originator. This default is configurable.

For a task that works on multiple devices, the default format of the email message subject is as follows:

```
$TaskName$ on group <device group name> completed with status $TaskStatus$
```

For example:

```
Take Snapshot on group Group1 completed with status Succeeded
```

For a task that works on multiple devices, the email message body contains a summary of the group task and a table of details for each child task associated with the group task. For more information, click the **View details of this task on HP NA** link.

For a task that works on multiple devices, the format of the email message body is not configurable.

An example group task completion email message follows:

```
Task Name: Take Snapshot
Task ID: 99701
Status: Succeeded
Comments:
Added by: Chris (Chris Admin)
Task Priority: 3
Create Date: 2013-01-22 20:02:56.0
Device Group: Group1
Schedule Date: As Soon As Possible
Start Date: As Soon As Possible
Complete Date: Tue Jan 22 20:03:16 MST 2013
Duration: 21
Repeat type: Non-recurring

View details of this task on HP NA (may not be available if the records were pruned)

Child tasks:
Succeeded       3
Failed          0
Skipped/Others  0
Total           3

Child task details:
Task  Task     Schedule   Host/Group     Task       Priority Partition  Scheduled  Comments
ID    Name     Date                      Status                         By

99711 Take     As Soon As  "TFastIronEdge Succeeded  3        Default    Chris
      Snapshot Possible    X424 Premium"                      Site       (Chris
                           (16.78.58.55)                                 Admin

99721 Take     As Soon As  lab-HPProc-540 Succeeded  3        Default    Chris
      Snapshot Possible    6zl                                Site       (Chris
                           (16.78.58.116)                                Admin)

99731 Take     As Soon As  ProCurveHPSwit Succeeded  3        Default    Chris
      Snapshot Possible    ch*4204*vl                         Site       (Chris
                           (16.78.58.138)                                Admin)
```

To change the default email message recipient, the format of the email message subject, or both for a group task, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. To change the default email message recipient, do the following:
   a. In the `adjustable_options.rcx` file, add the following line:

      ```
      <option name="task/email/recipient"></option>
      ```

   b. Insert a comma-separated list of email address recipients.

      To remove the default email message recipient, do not enter any email addresses. In this case, if the NA user who schedules the task neglects to enter an email address, the resulting message cannot be delivered.
3. To change the format of the email message subject, do the following:
   a. In the `adjustable_options.rcx` file, add the following line:

      ```
      <option name="grouptask/email/subject">$TaskName$ on group <device
      group name> completed with status $TaskStatus$</option>
      ```

   b. Edit the subject and text values. Table 19 on page 122 lists the available variables for use in these options.
4. Save the `adjustable_options.rcx` file.
5. Restart the NA services on all cores in the NA environment.

16 Configuring the Default Setting of the Force Save Check Box for New Tasks

For many NA device tasks, the Force Save task option specifies whether NA should overwrite the startup configuration with the current running configuration at the completion of the task. The setting applies to only those devices that support a startup configuration. The default value of this setting is configurable per task type in the `appserver.rcx` file.

For each device task, the `appserver.rcx` file contains an option in the following format:

```
<option name="DeviceInteraction/EnforceConfigurationSave/task_name">setting</option>
```

Possible values for *`task_name`* are:

- Take Snapshot
- Discover Driver
- Run ICMP Test
- Deploy Passwords
- Deploy Config
- Configure Syslog
- Run Command Script
- Run Diagnostics
- Synchronize Startup and Running
- Update Device Software
- Backup Device Software
- Reboot Device
- Run Device Script
- Delete ACLs
- VLAN Task
- Port Scan
- Add Device Context
- Remove Device Context
- OS Analysis
- Provision Device
- Batch Insert ACL Line
- Batch Remove ACL Line

Possible values for *setting* are:

- true—The Force Save field is visible for this task type and defaults to selected (overwrite the startup configuration). The user running the task can override the default setting by clearing the Force Save check box.
- false—The Force Save field is visible for this task type and defaults to cleared (do not change the startup configuration). The user running the task can override the default setting by selecting the Force Save check box.
- disabled—The Force Save field is not visible for this task type. The task will never attempt to overwrite the startup configuration with the running configuration.

To change the default setting of the Force Save check box for a specific device task type, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In the `appserver.rcx` file, locate the following line for the task that you want to change:

```
<option name="DeviceInteraction/EnforceConfigurationSave/task_name">setting</option>
```

3. Copy the line to change from the `appserver.rcx` file to the `adjustable_options.rcx` file.
4. In the `adjustable_options.rcx` file, edit the *setting* value.
5. Save the `adjustable_options.rcx` file.
6. Restart all NA services.
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

     `/etc/init.d/truecontrol restart`

The change takes effect for new tasks only.

17 Setting the Update Device Software Task Status to Reflect Child Task Status

Each Update Device Software task spawns child tasks (for example, the Discover Driver task). By default, the Update Device Software task status indicates the outcome of the software update work only.

As of NA 9.22.01, the status of the Update Device Software task can reflect the status of all spawned child tasks.

To enable this feature, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="deploy/child/warning">true</option>
   ```

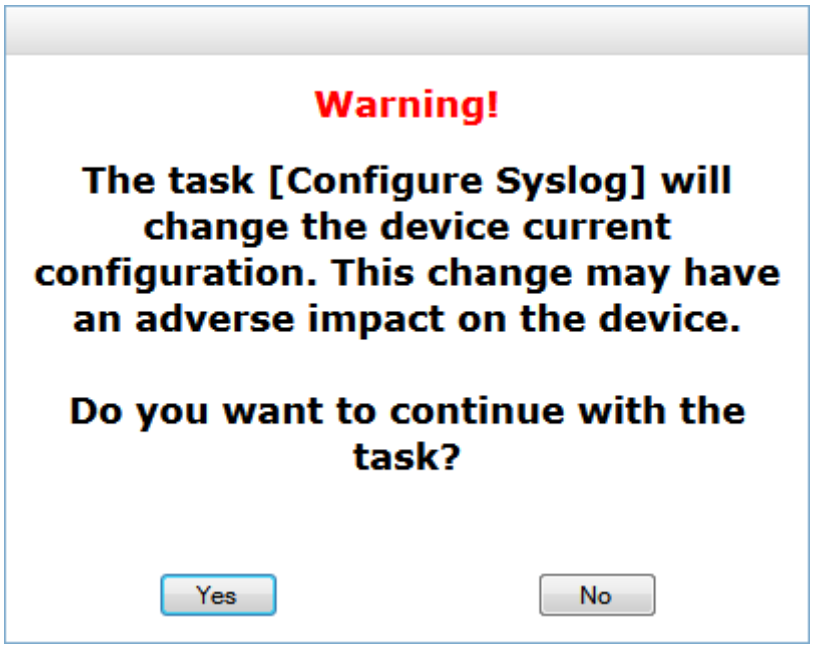
3. Save the `adjustable_options.rcx` file.
4. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - Restart the NA management engine.
5. In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

     ```
     /etc/init.d/truecontrol restart
     ```

18 Configuring NA to Warn Before a Task Modifies a Device

Many of the tasks available in NA change the configuration of the target devices. Some tasks also reboot devices, temporarily making them unavailable and changing the device configuration when the startup and running configurations differ. For a list of the tasks that change devices, see “What Are Tasks” in the *NA User Guide*.

By default NA completes these tasks as scheduled without reminding the user that the tasks impact device configurations.. As of NA 9.22.01, NA can warn that a task will change the target devices and give users a chance to cancel the task before it is scheduled. For example:



The warning appears for all users for all tasks that change the target devices.

The following exceptions apply:

- NA always warns before running the Reboot Device task regardless of the configuration described in this chapter.
- NA always warns before running the Update Device Software task. The warning message is more detailed when the configuration described in this chapter is enabled.

Alternatively, use the Workflow feature to require that a second person review and approve configured tasks before NA runs them. Workflow can be configured for some or all users, some or all task types, and some or all devices in the NA inventory.

To configure NA to display the warning message for tasks that change devices, follow these steps:

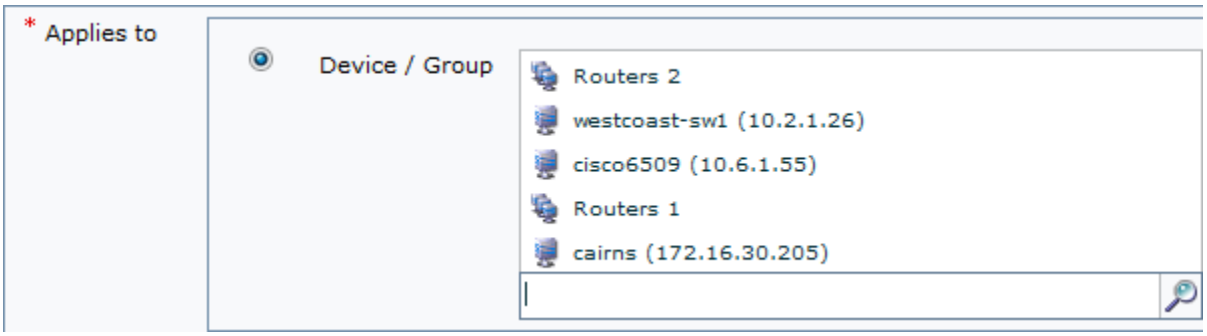
1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. Add the following line to the `adjustable_options.rcx` file:

   ```
   <option name="task/UI/WarnOnDeviceAlteringTask">true</option>
   ```

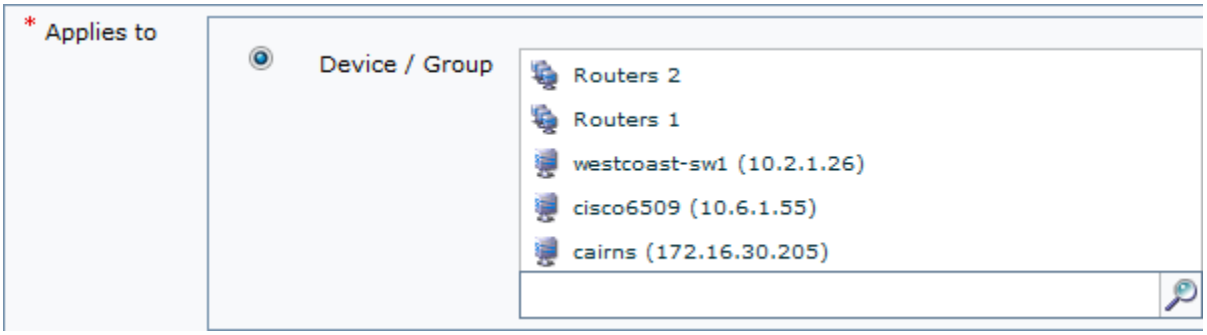
3. Save the `adjustable_options.rcx` file.
4. Reload the `.rcx` settings by doing *one* of the following:
   - In the NA console, on the Administrative Settings - User Interface page (**Admin > Administrative Settings > User Interface**), click **Save**.
   - Run the `reload server options` command from the NA proxy.
   - Restart the NA services.

19 Configuring NA to Sort Device Groups at the Top of the Applies To List

By default, the **Applies to** field in NA tasks displays the selected devices and device groups in the order of selection. With this behavior, devices and device groups can be intermingled in the selection list. For example:



As of NA 9.22.01, you can configure the **Applies to** field in NA tasks to display all selected device groups at the top of the list followed by all selected devices. Device groups appear in selection order followed by devices in selection order. For example:



To configure NA to display all device groups at the top of the list in the **Applies to** field, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. Add the following line to the `adjustable_options.rcx` file:

   ```
   <option name="flexui/devicechooser/sort_group_first">true</option>
   ```

3. Save the `adjustable_options.rcx` file.
4. Reload the `.rcx` settings by doing *one* of the following:
   - In the NA console, on the Administrative Settings - User Interface page (**Admin > Administrative Settings > User Interface**), click **Save**.
   - Run the `reload server options` command from the NA proxy.

- Restart the NA services.

20 Disabling the Use of Adobe Flash

HP Network Automation Software (NA) uses Adobe® Flash for displaying the device selector. If you disable the use of Flash, the NA console uses a pure HTML and JavaScript version of the device selector. Generally speaking, this version is slower than the Flash version because of the underlying protocol for communication between NA and the NA console, especially for large data sets (for example, 10,000 devices).

To disable the use of Adobe Flash in the NA console, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In the `appserver.rcx` file, locate the following line:

   ```
   <option name="flexui/devicechooser">true</option>
   ```

3. Copy the line from the `appserver.rcx` file to the `adjustable_options.rcx` file.
4. In the `adjustable_options.rcx` file, change the copied line to:

   ```
   <option name="flexui/devicechooser">false</option>
   ```

5. In the `adjustable_options.rcx` file, to control how many items the search box should return, add the following line:

   ```
   <option name="flexui/devicechooser/return_count">12</option>
   ```

   Optionally change the default value of 12 in this line.

   To reduce the number of search results, narrow the search pattern. For example, "192.168" might yield too many results to be displayed. Use "192.168.5" instead.

6. Save the `adjustable_options.rcx` file.
7. Restart all NA services.
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

     ```
     /etc/init.d/truecontrol restart
     ```

21 Setting the Preferred Credentials for Accessing a Device

NA administrators can configure the types of device credentials that NA uses for each task type. By default, this configuration is the same for all devices. Set this configuration in the Task Credentials section of the Administrative Settings - Device Access page (**Admin > Administrative Settings > Device Access**).

When a task type is configured for multiple device credential types, the user creating a task can select the device credential type to use for the task. The list of possible device credential types appears in the Device Credentials Options section of the task page.

As of NA 9.22.01, NA administrators can determine which device credential type takes precedence for a task on a per-device basis. This approach uses a custom field named Device Credentials (by default) that can be set for each device. Possible values are:

- (unset)—No preference. For each task, honor the user selection in the Device Credentials Options section of the task page. If this section is not available use the device credential type enabled on the Administrative Settings - Device Access page.
- User AAA—Always use the task owner's AAA credentials to access this device from any task type that enables user AAA credentials on the Administrative Settings - Device Access page.
- Standard—Always use the standard device-specific credentials or the first matching network-wide password rule to access this device from any task type that enables standard credentials on the Administrative Settings - Device Access page.

The precedence setting applies only when the task type permits the device credential type on the Administrative Settings - Device Access page. For example, consider:

- Device XYZ with User AAA as the preferred device credential type
- The Snapshot task type configured for both standard device credentials and user AAA credentials on the Administrative Settings - Device Access page
- The Run Command Script task type configured for standard device credentials on the Administrative Settings - Device Access page

In this case, NA behaves as follows:

- A Snapshot task against device XYZ uses the task owner's AAA credentials to access the device. NA ignores the selection in the Device Credentials Options section of the task page.
- A Run Command Script task against device XYZ uses the standard device-specific credentials or the first matching network-wide password rule to access the device. This task does not use AAA credentials, because that option is not enabled on the Administrative Settings - Device Access page.

To enable the specification of preferred credentials for a device, follow these steps:

1. Change to the directory that contains the `.rcx` files:
   - *Windows*: `<NA_HOME>\jre`
   - *Linux*: `<NA_HOME>/jre`
2. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
3. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="per_device/task_credentials/enabled">true</option>
   ```
4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing one of the following:
   - Run the `reload server options` command from the NA proxy.
   - On the User Interface page (**Admin > Administrative Settings > User Interface**) of the NA console, click Save.
   - Restart the NA management engine.
6. In the NA console, open the Custom Data Setup page (**Admin > Custom Data Setup**).
7. From the **Custom Data Setup** list, choose `Devices`.
8. Select the the check box for an unused custom field, and then enter the following values:
   a. Set **API Name** to `devicecreds`.
   b. Set **Display Name** to `Device Credentials`.
   c. For the **Values** field:
      — Clear the **Can Contain HTML** check box.
      — Select the **Limit to** check box, and then enter `User AAA,Standard`.
   d. Click **Save**.

The display name appears in the NA console. You can customize it for your environment.

The API name and limiting values are embedded in the NA code. Use the exact strings listed here.

To set the preferred credentials for a device, follow these steps:

1. Navigate to the device details page.
2. From that page, open the Edit Device page (**Edit > Edit Device**).
3. In the Additional Information section, select a value for the **Device Credentials** field (or the customized display name that corresponds to the devicecreds API name.

22 Configuring the Diagnostic Policy Compliance Check Setting Default

Prior to NA 9.22, when the output of a Run Diagnostics task differed from the output of the previous diagnostic for a device, NA always initiated the diagnostic policy rules for the policy checks associated with that device. Such action can result in a large number of Check Policy Compliance tasks.

As of NA 9.22, this behavior is configurable on a per task basis with the **Run compliance check when change detected** check box. By default, this check box is selected. This default setting mirrors the behavior prior to NA 9.22.

To change default setting of the **Run compliance check when change detected** check box to unselected, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In the `adjustable_options.rcx` file, add the following line:

```
<option name="Device/Diagnostics/RunComplianceCheckDefault">false</option>
```

3. Save the `adjustable_options.rcx` file.
4. Restart all NA services.
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

     `/etc/init.d/truecontrol restart`

The change takes effect for new tasks only.

23 Parsing Cisco ACS 5.x Logs for Change Detection

As of version 9.20, HP Network Automation Software (NA) provides a mechanism for parsing Cisco Secure Access Control System (ACS) 5.x logs for change detection when those logs are forwarded by ACS 5.x to the NA Syslog server.

The NA AAA Log Reader Agent cannot be used to process ACS 5.x logs because ACS 5.x uses a format different from that of standard RFC-compliant logs. Also, the NA AAA Log Reader Agent is a Windows application while ACS 5.x is installable on a Cisco Secure ACS appliance or VMware.

To enable the use of ACS 5.x logs for change detection, follow these steps:

1. Configure the ACS 5.x server to forward ACS logs to the NA syslog server:
   a. On ACS 5.x, use System Administration > Log Configuration > Remote Log Targets > Create to set the IP address of the NA Syslog server.

      Use Advanced Syslog Options to verify that the Port and Facility Code values match the configuration of the NA Syslog server.

   b. On ACS 5.x, use System Administration > Log Configuration > Log Categories > Global (or Per Instance) to set the categories of logs to be forwarded (for example, AAA Audit).

      For the selected categories, use the Remote Log Target tab to add the NA Syslog server configured in the previous step as a target.

      For more information, see:

      http://www.cisco.com/en/US/products/ps9911/products_user_guide_list.html
2. On the NA server, update the syslog configuration
   a. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
   b. In the `appserver.rcx` file, locate the following line:

      ```
      <option name="syslog/process_other_treatments">false</option>
      ```
   c. Copy the line from the `appserver.rcx` file to the `adjustable_options.rcx` file.
   d. In the `adjustable_options.rcx` file, change the copied line to:

      ```
      <option name="syslog/process_other_treatments">true</option>
      ```
   e. Save the `adjustable_options.rcx` file.

3 Restart all NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  ```
  /etc/init.d/truecontrol restart
  ```

4 In the NA console, go to Admin > Administrative Settings > Configuration Mgmt, and then add the pattern "CSCOacs" to the Syslog Detection Patterns list.

24 Extending the Number of Custom Enhanced Fields

In the NA console, you can configure up to 31 custom data fields each for the Device Details page and the Device Interfaces page. These fields are available as follows:

- Six fields can be configured on the Admin > Custom Data Setup page.
- 25 fields can be configured on the Admin > Enhanced Custom Fields Setup page (when the Enable Enhanced Custom Fields check box is selected on the Admin > Administrative Settings > User Interface page).

To extend the available number of enhanced custom fields for the Device Details page, the Device Interfaces page, or both pages, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In a text editor, such as Word or vi, edit the `adjustable_options.rcx` file as follows:
   - To extend the number of enhanced custom fields for the Device Details page, add the following line:

     ```
     <option name=" metadata/field_limit/RN_DEVICE">100</option>
     ```

   - To extend the number of enhanced custom fields for the Device Interfaces page, add the following line:

     ```
     <option name=" metadata/field_limit/RN_DEVICE_PORT">100</option>
     ```

To restrict the number of available enhanced custom fields, replace 100 with a smaller value. (Specifying a larger value has the same effect as the leaving the value at 100.)

3. Save the `adjustable_options.rcx` file.
4. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - Restart the NA management engine.

25 Configuring NA to Run Windows PowerShell Scripts

The Windows PowerShell scripting language is widely available on Windows operating systems. Windows PowerShell commands, called cmdlets, are instances of .NET Framework classes. Cmdlets can use the HP Network Automation Software (NA) SOAP API to interact with NA data. You can call these NA-related cmdlets from NA advanced scripts. Additionally, you can call cmdlets and the NA SOAP API functions directly from the Windows PowerShell prompt.

As of version 9.22.01, NA supports Windows PowerShell as an advanced scripting language. All Windows PowerShell script names must use the `ps1` file name extension.

To configure NA to correctly interpret and run Windows PowerShell scripts, follow these steps:

1. On *each* NA core, configure NA to understand the `ps1` file name extension.
   a. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
   b. In the `adjustable_options.rcx` file, add the following line:

      ```
      <option name="apprunner/temp_file_extension">ps1</option>
      ```

   c. Save the `adjustable_options.rcx` file.
   d. Reload the .rcx settings by doing one of the following:
      — Run the `reload server options` command from the NA proxy.
      — Restart the NA services.
2. In the NA console, add Windows PowerShell as an advanced scripting language.
   a. Open the Administrative Settings - Server page (**Admin > Administrative Settings > Server**).
   b. Under Advanced Scripting, identify the next available scripting language (3 by default).
   c. For Scripting Language x, enter **`PowerShell`**.
   d. For Path to Interpreter x, enter the absolute path, including the executable, to `PowerShell.exe` on the NA server.
   e. Click **Save**.

To use a Windows PowerShell script in NA, on the New Command Script page, select the **Advanced Scripting** check box, and then for **Language** select PowerShell. For more information about command scripts, see the help for the New Command Script page.

Troubleshooting

On the Task Information page for a command script task, an error similar to this example indicates that Windows PowerShell is not enabled run scripts:

```
Created temporary file
C:\Windows\system32\config\systemprofile\AppData\Local\Temp\
t160232884.ps1
Executing command:
c:\windows\system32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\system32\config\systemprofile\AppData\Local\Temp\
t160232884.ps1
File C:\Windows\system32\config\systemprofile\AppData\Local\Temp\
t160232884.ps1
cannot be loaded because the execution of scripts is disabled on this
system.
Please see "get-help about_signing" for more details.
```

To enable Windows PowerShell for running scripts, run the following command at the Windows PowerShell prompt on the NA server:

```
Set-ExecutionPolicy RemoteSigned
```

For more information, see:

http://technet.microsoft.com/en-us/library/hh849812.aspx

More Information

For information about the cmdlets included with Windows PowerShell, see:

http://technet.microsoft.com/en-us/library/dd347730.aspx

For information about writing custom cmdlets, see:

http://msdn.microsoft.com/en-us/library/windows/desktop/dd878294(v=vs.85).aspx

26 Customizing the Banner on the NA SSH Server

As of NA 9.22.01, you can customize the banner that the NA SSH server displays when an SSH session is initiated.

To enable this feature, follow these steps:

1. Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.
2. In the `adjustable_options.rcx` file, add the following line:

   ```
   <option name="proxy/ssh_banner">BANNER_TEXT</option>
   ```

3. Replace `BANNER_TEXT` with plain text. To create a multi-line banner, enter a carriage return at the end of each line. For example:

   ```
   <option name="proxy/ssh_banner">THIS IS A BANNER WITH SEVERAL LINES
   BANNER LINE2
   BANNER LINE3</option>
   ```

4. Save the `adjustable_options.rcx` file.
5. Reload the `.rcx` settings by doing *one* of the following:
   - Run the `reload server options` command from the NA proxy.
   - Restart the NA management engine.
6. In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

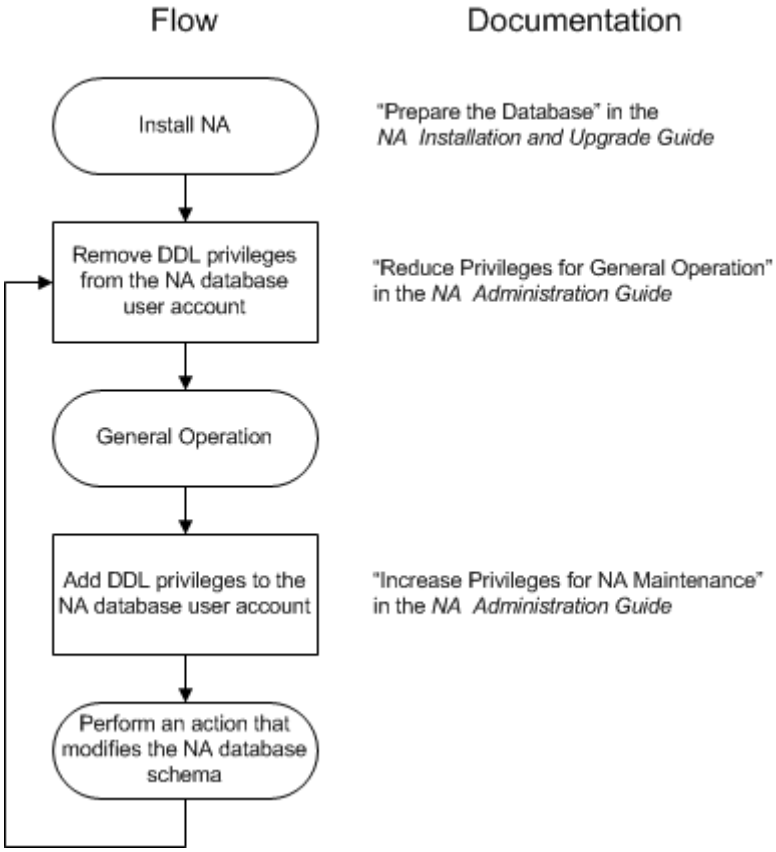
     ```
     /etc/init.d/truecontrol restart
     ```

27 Running NA with Minimal Database User Privileges

For general operation, the database user account that accesses the HP Network Automation Software (NA) database requires only data manipulation language (DML) privileges. However, some database maintenance operations (including upgrading NA) require that the database user account have data definition language (DDL) privileges.

The diagram in Figure 5 presents an overview of the privileges needed on the NA database user account at various points in time.

Figure 5 Database Privileges Flow



This chapter describes how to reduce database user account privileges after NA installation and how to increase those privileges for database maintenance operations. It contains the following topics:

- Reduce Privileges for General Operation on page 148
- Increase Privileges for NA Maintenance on page 151

For information about the database user account privileges required for initial NA installation, see "Prepare the Database" in the *NA Installation and Upgrade Guide*.

Reduce Privileges for General Operation

For general NA operation, the database user account requires only DML privileges and not DDL privileges. After NA installation or maintenance, you can reduce the privileges granted to the NA database user account.

Reducing Privileges for Oracle

Complete this procedure any time you want to limit the NA database user account privileges.

With Oracle, revoke the following DDL privileges from the NA database user:

- CREATE SEQUENCE
- CREATE SESSION
- CREATE TABLE
- CREATE PROCEDURE
- SELECT ANY DICTIONARY
- ALTER ANY TABLE
- DROP ANY TABLE
- CREATE ANY INDEX
- ALTER ANY INDEX
- DROP ANY INDEX

For example (for Oracle user name `nauser`):

```
REVOKE CREATE SEQUENCE,CREATE SESSION, CREATE TABLE, CREATE PROCEDURE from nauser;
REVOKE SELECT ANY DICTIONARY, ALTER ANY TABLE, DROP ANY TABLE from nauser;
REVOKE CREATE ANY INDEX, ALTER ANY INDEX, DROP ANY INDEX from nauser;
```

After revoking the DDL privileges, the following DML privileges remain on the NA database user:

- CONNECT
- SELECT ANY TABLE
- INSERT ANY TABLE
- UPDATE ANY TABLE
- DELETE ANY TABLE
- UNLIMITED TABLESPACE
- EXECUTE on CTXSYS.ctx_ddl

Reducing Privileges for SQL Server

The procedure for restricting database access depends on account history. For more information about specific use cases, see each procedure:

- First Time Modification on page 149
- Subsequent Modification on page 150

First Time Modification

Complete this procedure the first time you want to limit the NA database user account privileges. This procedure removes the `db_owner` role from the NA database user account. This action removes all privileges from the account. The procedure then sets DML privileges on the account by initially re-adding all privileges and then removing DDL privileges.

To modify the SQL Server NA database user account to set privileges for general NA operation, follow these steps (for SQL Server user name `nauser`):

1. Stop all NA services.
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

     ```
     /etc/init.d/truecontrol stop
     ```
2. Log on to SQL Server as a SQL Server administrator user with the `sysadmin` role (for example, SA).
3. Remove the `db_owner` role from the NA database user account.
   a. In Microsoft SQL Management Studio, right-click **`nauser`**, click Properties, and then click **User Mapping**.
   b. Under **Users mapped to this login**, select the NA schema.
   c. Under **Database role membership for <NA schema>**, clear the **db_owner** check box.
   d. Click **OK**.

   At this point, the NA database user account has no privileges and cannot access SQL Server.
4. Set permissions for the NA database user account.
   a. Give access to the NA database user account. For example:

      ```
      use NA; GRANT CONTROL to nauser; go
      ```

      This command returns all privileges associated with the `db_owner` role.
   b. Remove the schema modification privileges from the NA database user account. For example:

      ```
      use NA; DENY ALTER to nauser; go
      ```

This command retains read and write privileges for the NA database user account.

c *Optional*. Verify the permissions required by the NA schema. For example:

```
SELECT * FROM fn_my_permissions(NULL, 'DATABASE') order by
permission_name;
```

This command lists the 18 permissions provided to the NA schema.

d *Optional*. Verify the permissions granted to the NA database user account. For example:

```
EXEC sp_helprotect NULL, 'nauser';
```

5 Start all NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol start
```

Subsequent Modification

Complete this procedure sometime after using the `REVOKE ALTER` command to re-add DDL privileges to the NA database user account.

To remove the DDL privileges from the NA database user account that does not have the `db_owner` role, follow these steps:

1 Log on to SQL Server as a SQL Server administrator user with the `sysadmin` role (for example, SA).

2 Remove the schema modification privileges from the NA database user account. For example:

```
use NA; DENY ALTER to nauser; go
```

Increase Privileges for NA Maintenance

The following NA maintenance scenarios require DDL privileges:

- Upgrading NA by running a service pack installer (SPI)
- Applying an NA patch or hotfix that changes the NA database schema
- Enabling case-insensitive search or full-text search; this enablement modifies the NA database schema

The information in this section restores to the NA database user the privilege level used to create the NA database tables. After completing NA maintenance, you can follow the steps in Reduce Privileges for General Operation on page 148 to remove the DDL privileges.

Increasing Privileges for Oracle

Complete this procedure to re-add DDL privileges to the NA database user account after following the procedure in Reducing Privileges for Oracle on page 148.

With Oracle, grant the following DDL privileges to the NA database user:

- CREATE SEQUENCE
- CREATE SESSION
- CREATE TABLE
- CREATE PROCEDURE
- SELECT ANY DICTIONARY
- ALTER ANY TABLE
- DROP ANY TABLE
- CREATE ANY INDEX
- ALTER ANY INDEX

For example (for Oracle user name `nauser`):

```
GRANT CREATE SEQUENCE,CREATE SESSION, CREATE TABLE, CREATE PROCEDURE to nauser;
GRANT SELECT ANY DICTIONARY to nauser;
GRANT ALTER ANY TABLE, DROP ANY TABLE to nauser;
GRANT SELECT ANY DICTIONARY, ALTER ANY TABLE, DROP ANY TABLE to nauser;
GRANT CREATE ANY INDEX, ALTER ANY INDEX to nauser;
```

After granting DDL privileges, the NA database user has the privileges listed in "Oracle Database Options" in the *NA Installation and Upgrade Guide* version 9.22 or later.

Increasing Privileges for SQL Server

Complete this procedure to re-add DDL privileges to the NA database user account after following either of the procedures in Reducing Privileges for SQL Server on page 149.

To modify the SQL Server NA database user account to grant DDL privileges to the NA database user account, follow these steps (for SQL Server user name `nauser`):

1. Log on to SQL Server as a SQL Server administrator user with the `sysadmin` role (for example, SA).
2. Grant database modification privileges to the NA database user account. For example:

```
use NA; REVOKE ALTER to nauser; go
```

28 Changing NA Credentials When Connecting to a New Database Location

If the NA database has been moved to a different server, use the tc_tools utility to configure NA to connect to the new database location. This location must include a valid NA database. For information about installing the NA database, see the *NA Installation and Upgrade Guide* or consult your database administrator.

The tc_tools utility updates the following information on the NA server:

- Database server name
- Database port
- Database name
- Database username
- Database user password

To connect NA to a different NA database, follow these steps:

1. At a command prompt, run the following command:
   - Windows: `<installdir>\client\tc_tools.bat`
   - UNIX: `<installdir>/client/tc_tools.sh`
2. Type **1** to change the database connection information.
3. At each prompt, do *one* of the following:
   - Type the new value for the prompt.
   - Press **Enter** to retain the value between the brackets ([ ]).
4. From the `tc_tools` prompt, exit the utility.
5. Restart the NA management engine.

29 Full-Text Search of Configuration Text (Oracle and SQL Server)

HP Network Automation Software (NA) supports a contains (full text) search of Configuration Text. After full-text search is enabled, faster configuration text search is available for the following report options:

- Reports > Search For > Devices > Configuration Text > contains (full text)
- Reports > Search For > Configurations > Configuration Text > contains (full text)
- Reports > Search For > Device Templates > Configuration Text > contains (full text)
- Reports > Advanced Search > Search Criteria > Configuration Text > contains (full text)

Additionally, you can create a dynamic group or a dynamic policy scope based on the results of a Search Criteria > Configuration Text > contains (full text) search.

Similarly, these searches also support searching for configuration text that does not contain (full text). The search is always case insensitive for the contains (full text) and does not contain (full text) operators.

The contains (full text) search is an indexed search and requires that the database is enabled for full-text search.

Because the contains (full text) search is indexed, it returns results faster than does the contains search. However, the contains (full text) search supports fewer options than does the contains search. For information about the supported options, see "Using the Full-Text Search Functionality" in the NA help or the *NA User Guide*.

This feature is not supported on MySQL.

This topic contains the following topics:

Enabling Full-Text Search of Configuration Text

Full-text search accesses an index of the text records in the database. The initial index generation requires available time and disk space.

If Oracle Text (for an Oracle database) or the SQL Server Full Text Search service (for a Microsoft SQL Server database) is not yet enabled, also plan for database downtime.

NA maintains the full text index by incrementally indexing new configurations added during snapshot tasks and by removing the index entries of deleted configurations.

Note the following:

- Because index generation is CPU-intensive, NA tasks might run slower than normal during the process of enabling full text search.
- Do not restart the NA management engine while index generation is in progress.

In a Horizontal Scalability environment, enable full-text searching on *one* NA server.

In a Multimaster Distributed System environment, enable full-text searching on *each* NA server. Run the enablement procedures in parallel. That is, complete step 1 on each NA server before initiating step 2 on any NA server, and so forth.

Follow the steps appropriate to the database type:

- Enabling Full-Text Search on Oracle on page 157
- Enabling Full-Text Search on Microsoft SQL Server on page 159

Enabling Full-Text Search on Oracle

To enable full-text search on an Oracle database, follow these steps:

1. Verify that Oracle Text is enabled and has the required privileges and space:
   a. Log on to the NA proxy with the credentials used to install NA.
   b. Run the following command:

      ```
      fulltextsearch -option analyze
      ```

   c. Examine the output of the analyze command.
      — If Oracle Text is not enabled, engage the Oracle database administrator to change the configuration. For information about enabling Oracle Text, see "Administering Oracle Text" in the *Oracle Text Application Developer's Guide*.

      Another information source is the Oracle MetaLink document collection, for which you must have a MetaLink account with Oracle. Documents of interest include the following:
      – 280713.1: *Manual installation, deinstallation of Oracle Text 10gR1*
      – 979705.1: *Manual installation, deinstallation of Oracle Text 10gR2*
      – 579601.1: *Manual installation, deinstallation and verification of Oracle Text 11gR1*
      – 970473.1: *Manual installation, deinstallation and verification of Oracle Text 11gR2*

      — If Oracle Text is enabled, do the following:
      – Determine whether data pruning is needed. If the analyze command output recommends database pruning, complete this process before generating the full-text index. For more information, see "Data Pruning" in the *NA Installation and Upgrade Guide*.
      – Verify that the approximate additional space required for the index generation process is available on the database server.

        The index configuration process requires available disk space of 50% to 200% of the configuration text size. Actual space requirements depend on the database contents.

        The index configuration process is resource-intensive. Actual time depends on database hardware and configuration as well as the volume of text to be indexed.

        For more information, see "Frequently Asked Questions About Indexing Performance" in the *Oracle Text Application Developer's Guide*.
      – Consider the approximate time required for the index generation process. The analyze command calculates time based on the use of a single thread. You can reduce this time by using multiple threads while generating the index. To figure the adjusted approximate time, divide the suggested time by the number of threads that will be used in step 3.
2. In the NA console, delay any Take Snapshot tasks that are scheduled to start before the end of the approximate time required for index generation to complete.

3 Generate the full-text index:

a From the NA proxy, run the following command:

```
fulltextsearch -option enable -numthreads T
```

T is the number of parallel threads. Possible values range from 1 to one less than the number of database server cores.

b Examine the output of the enable command.

— The expected status is COMPLETE & VALID.

— If the status is IN PROGRESS, wait for index generation to complete.

— If the status is INVALID, remove the index with the `fulltextsearch -option disable` command, and then repeat step a.

You can close the command prompt window during index generation. In this case, run the following command to determine the status of the index generation:

```
fulltextsearch -option status
```

Alternatively, you can watch the NA logs with the troubleshooting option feature/proxy set to debug.

4 In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

5 In the NA console, examine the status of recent Take Snapshot tasks. Rerun any that failed.

On an Oracle database, the log file contains an error for any Take Snapshot tasks that were running during the generation of the full text index. You can ignore the following error:

```
java.sql.SQLException: ORA-29861: domain index is marked LOADING/
FAILED/UNUSABLE
```

Enabling Full-Text Search on Microsoft SQL Server

To enable full-text search on a Microsoft SQL Server database, follow these steps:

1. Verify that the SQL Server Full Text Search service is enabled and has the required privileges:
   a. Log on to the NA proxy with the credentials used to install NA.
   b. Run the following command:

      ```
      fulltextsearch -option analyze
      ```

   c. Examine the output of the analyze command.
      — If the SQL Server Full Text Search service is not enabled, engage the SQL Server database administrator to change the configuration.
      — If the SQL Server Full Text Search service is enabled, determine whether data pruning is needed. If the analyze command output recommends database pruning, complete this process before generating the full-text index. For more information, see "Data Pruning" in the *NA Installation and Upgrade Guide*.
2. On SQL Server 2005, remove the SQL Server noise words as follows:
   a. Change to the `$SQL_Server_Install_Path\Microsoft SQL Server\MSSQL.1\MSSQL\FTDATA\` directory.
   b. Back up the `noiseENU.txt` file.
   c. Delete all entries in the `noiseENU.txt` file to leave an empty file.

   For more information about editing noise words, see the "Noise Words" topic in the MSDN library:

   http://msdn.microsoft.com/en-us/library/ms142551(v=sql.90).aspx

   On SQL Server 2008, by default no noise words are enabled.
3. Generate the full-text index:
   a. Log on to the NA proxy with the credentials used to install NA.
   b. Run the following command:

      ```
      fulltextsearch -option enable
      ```

   On SQL Server, this command returns immediately and starts full-text indexing. Wait some time before you start using the new search. In the output, verify that this run did not generate any SQL exceptions.
4. Determine the status of the index generation by running the following command:

   ```
   fulltextsearch -option status
   ```

   - The expected status is COMPLETE & VALID.
   - If the status is IN PROGRESS, wait for index generation to complete.
   - If the status is INVALID, remove the index with the `fulltextsearch -option disable` command. If necessary, increase the available disk space, and then repeat step 3.

   Alternatively, you can watch the NA logs with the troubleshooting option feature/proxy set to debug.

5 In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  `/etc/init.d/truecontrol restart`

Adding a Reminder to Use Full-Text Search Where Applicable

As of NA 9.22.01, NA supports adding a custom message to the Configuration Text field on the applicable search pages. The message describes when NA users should use the contains (full text) search operator. The message is the same for all Configuration Text fields and is visible only when full-text search is enabled.

To add a message to the Configuration Text fields, follow these steps:

1 Change to the directory that contains the `.rcx` files:

- *Windows*: `<NA_HOME>\jre`
- *UNIX*: `<NA_HOME>/jre`

2 Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.

3 In the `adjustable_options.rcx` file, add the following line:

```
<option name="fulltextsearch/warning_msg">HTML_formatted_text</option>
```

4 Replace `HTML_formatted_text` with text formatted in an HTML table cell and the span identifier `fulltextwarning`. For example:

```
<option name="fulltextsearch/warning_msg">
<![CDATA[<td><span id="fulltextwarning">For faster search results, use
the contains (full text) and does not contain (full text) operators.
For supported search options, see <a class="help" href="#" onclick="var
hw = window.open('tcdocs/en/wwhelp/wwhelp/wwhimpl/common/html/
wwhelp.htm?context=Online_Help&amp;file=Ch11a2.html#wp205730','WWHFram
e','scrollbars=yes,alwaysRaised=yes,resizable=yes,dependent=yes');
hw.focus(); return false;">Using the Full-Text Search Functionality</a>
in the NA help.</span></td>]]>
</option>
```

5 Save the `adjustable_options.rcx` file.

6 Reload the `.rcx` settings by doing *one* of the following:

- Run the `reload server options` command from the NA proxy.
- Restart the NA management engine.

7 In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  ```
  /etc/init.d/truecontrol restart
  ```

Disabling Full-Text Search

In a Horizontal Scalability environment, disable full-text searching on *one* NA server.

In a Multimaster Distributed System environment, disable full-text searching on *each* NA server. Run the disablement procedures in parallel. That is, complete step 1 on each NA server before initiating step 2 on any NA server, and so forth.

To permanently disable the contains (full text) search operator in the NA console and to remove the full-text index from the database, follow these steps:

1 If any dynamic groups are configured to use the contains (full text) or does not contain (full text) operator, edit or delete these dynamic group configurations.

2 If any dynamic policy scopes are configured to use the contains (full text) or does not contain (full text) operator, edit or delete these dynamic policy configurations.

3 Remove the full-text index:

a Log on to the NA proxy with the credentials used to install NA.

b Run the following command:

```
fulltextsearch -option disable
```

4 Disable the full-text search feature by removing the contains (full text) and does not contain (full text) operators from the NA console:

a Change to the directory that contains the `.rcx` files:

- *Windows*: `<NA_HOME>\jre`
- *UNIX*: `<NA_HOME>/jre`

b Back up the `adjustable_options.rcx` file to a location outside the `<NA_HOME>` directory.

c In the `adjustable_options.rcx` file, add the following line:

```
<option name="fulltextsearch/enabled">false</option>
```

d Save the `adjustable_options.rcx` file.

e Reload the `.rcx` settings by doing *one* of the following:

— Run the `reload server options` command from the NA proxy.

— Restart the NA management engine.

5 In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

30 Enabling Case-Insensitive Search (Oracle)

HP Network Automation Software (NA) supports case-insensitive searches of many objects in the NA database on Oracle. (The MySQL and Microsoft SQL Server database searches are already case-insensitive.)

This topic contains the following sections:

Affected Fields

When enabled, case-insensitive search is available for most text fields in the NA console, as described here. Additionally, as of NA 9.20 Patch 1, the command-line interface is case-insensitive for device hostname.

Search Box

The IP or Hostname search box follows the case-sensitivity configuration.

Search Criteria

The Search Criteria field is available for the following functions:

- Defining a dynamic device group on the New Group and Edit Group pages.
- Defining a dynamic policy scope on the New Policy and Edit Policy pages.
- Creating a custom search on the Advanced Search page.

With an Oracle database, case-insensitive search is not available for the following fields:

- ACL Application
- ACL Configuration
- Comments
- Configuration Text with the contains and does not contain operators. (The contains (full text) and does not contain (full text) operators are always case-insensitive.)

All other fields follow the case-sensitivity configuration.

Device Selector

For the New Task and Rerun Task pages, the Filter box on the device selector follows the case-sensitivity configuration.

Reports

Table 20 lists the report fields that can be searched on a case-insensitive basis when the case-insensitive search feature is enabled.

Table 20 Case Sensitivity of Report Search Fields

Search Type	Case-Insensitive Fields		Case-Sensitive Fields
Device	• Host Name • Device Vendor • Device Model • FQDN • Access Methods • Device Location • Serial Number • Asset Tag • Device Software Version • Device Firmware Version • Device Description • Password Rule • ACL ID • ACL Handle	• ACL Type • Module Slot • Module Description • Module Model • Module Serial • Module Firmware Version • Module Hardware Revision • ROM Version • Service Type • Custom Service Type • VTP Domain Name • VTP Operating Mode	• Comments • Configuration Text • ACL Configuration • ACL Application
Interface	• Port Name • Port Type • Port Status • Running Port State • Description • Configured Duplex • Configured Speed • Negotiated Duplex	• Negotiated Speed • VLAN Name • Host Name • Module Slot • Module Description • Module Model • Module Serial • Module Firmware Version	
Module	• Host Name • Module Slot • Module Description • Module Model	• Module Serial • Module Firmware Version • Module Hardware Revision	• Comments
Policy	• Policy Name • CVE	• Vendor URL • Solution URL	• Solution
Policy, Rule, and Compliance	• Host Name	• CVE	

Table 20 Case Sensitivity of Report Search Fields (cont'd)

Search Type	Case-Insensitive Fields		Case-Sensitive Fields
Configuration	• Host Name	• Changed By	• Comments • Configuration Text
Diagnostic	• Host Name		• Diagnostic Text
Task	• Task Name • Host Name	• Scheduled By	• Comments • Result
Session	• Host Name	• Created By	• Session Data
Event	• Added By	• Host Name	• Description
User	• First Name • Last Name • User Name	• Email Address • AAA User Name • Comments	
ACL	• Host Name • ACL ID • ACL Handle	• ACL Type • Changed By	• ACL Configuration • ACL Application • Comments
MAC Address	• Host Name • Port Name	• Port Description • VLAN	
IP Address	• Host Name • Port Name • Port Description	• VLAN • Associated MAC	
VLAN	• Host Name • VLAN Name • VLAN Type	• VLAN Description • Private VLAN	
Device Template	• Template Name • Device Vendor	• Device Model • Device Description	• Comments • Configuration Text
Single Search	• Added By • Host Name	• Description	

Enabling Case-Insensitive Search of an Oracle Database

For an Oracle database, case-insensitive search accesses a case-insensitive index of the text records in the database for each field in the query.

In a Horizontal Scalability environment, enable case-insensitive searching on *one* NA server.

In a Multimaster Distributed System environment, enable case-insensitive searching on *each* NA server.

To enable case-insensitive search of NA with an Oracle database, follow these steps to generate the case-insensitive indexes:

1. Connect to the NA proxy with the credentials used to install NA.
2. Run the following command:

   ```
   mod oraclecaseinsensitive -option enable
   ```

   As of NA 9.20 Patch 1, running this command triggers a recalculation of dynamic group membership.

3. In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:

   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

     ```
     /etc/init.d/truecontrol restart
     ```

Disabling Case-Insensitive Search

In a Horizontal Scalability environment, disable case-insensitive searching on *one* NA server.

In a Multimaster Distributed System environment, disable case-insensitive searching on *each* NA server.

To permanently disable case-insensitive search of NA with an Oracle database and to remove the case-insensitive indexes from the database, follow these steps:

1. If any dynamic groups are configured with case-insensitive search criteria, edit or delete these dynamic group configurations.
2. If any policies are configured with case-insensitive search criteria, edit or delete these policy configurations.
3. Remove the case-insensitive indexes:
   a. Connect to the NA proxy with the credentials used to install NA.
   b. Run the following command:

      ```
      mod oraclecaseinsensitive -option disable
      ```

      As of NA 9.20 Patch 1, running this command triggers a recalculation of dynamic group membership.
4. In a Horizontal Scalability environment, synchronize the database configuration by restarting NA on all other NA servers connected to the NA database:
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

     ```
     /etc/init.d/truecontrol restart
     ```

31 Reclaiming Unused Space (Oracle)

Database maintenance often involves deleting data chunks within a database table, which results in free space inside the table. New records added after this maintenance populates the free space inside the table first, so the new records can be spread across several physical locations within the table. This fragmentation degrades database performance by extending data access times.

HP Network Automation Software (NA) pruning tasks can cause database table fragmentation. This section identifies one way to defragment an Oracle database tablespace. This procedure can be performed while the database is online.

This documentation describes one approach to this database administration task. Read the prerequisites to determine whether this approach applies to your situation. For other approaches and more detailed information, see the documentation for your database type and version.

Tablespace defragmentation can be run against all tables in the NA schema. Table 21 lists the NA database tables and the associated LOB columns that are most frequently affected by fragmentation.

Table 21 NA Database Tables Frequently Affected by Fragmentation

Table Name	Target LOB Columns
RN_DEVICE_ACCESS_LOG	• ChangeEventData • Comments
RN_DEVICE_DATA	• DataBlock • Comments
RN_DEVICE_TOPOLOGY_DATA	
RN_DIAGNOSTIC_DATA	• DataBlock • Comments
RN_EVENT	• EventText • EventData
RN_EVENT_MESSAGE	• MessageBody
RN_SCHEDULE_TASK	• Comments • Result • TaskData

To defragment an Oracle database tablespace, follow these steps:

1. Verify that the tablespace meets the following prerequisites:
   - The tablespace must be set with automatic segment space management (ASSM).
   - The disk space available to the redo log must be sufficiently large relative to the size of the tablespace.
2. Enter the SQL*Plus command-line interface as the SYSDBA user.
3. Use the Oracle Segment Advisor to determine whether defragmentation is needed. Either check the results of the Automatic Segment Advisor or run the Segment Advisor manually.

   For more information, see "Using the Segment Advisor" in the *Oracle Database Administrator's Guide*.
4. For each table that requires defragmentation, do the following:
   a. Enable row movement by running the following command:

      ```
      ALTER TABLE <table_name> ENABLE ROW MOVEMENT;
      ```

   b. Reclaim unused rows by running the following command:

      ```
      ALTER TABLE <table_name> SHRINK SPACE;
      ```

   c. Reclaim unused LOB columns by running the following command:

      ```
      ALTER TABLE <table_name> MODIFY LOB (<lob_column_name>) (SHRINK SPACE);
      ```

Alternatively, reclaim unused rows and columns with one command as follows:

```
ALTER TABLE <table_name> SHRINK SPACE CASCADE;
```

This CASCADE command replaces step b and step c.

32 Restoring Databases

Oracle

For information on restoring Oracle databases, see your Oracle database administrator.

SQL Server

To restore a Microsoft SQL Server database:

1. Make a backup of the database you are about to restore.
2. Launch SQL Server Management Studio.
3. Connect to the SQL Server database server and navigate to your database.
4. Right-click the database, and then select Tasks > Restore > Database.
5. Click the Restore: From Device button.
6. Click Select Devices.
7. Click Add.
8. Open the file browser under File name and select the filename you want to restore.
9. Click OK three times.
10. Click the Options tab.
11. Select Force restore over existing database.
12. Click OK. The database should be restored.

If you receive an error message, such as “Database is in use,” you need to either close the connection to that database (stop the jboss server), or go to the Options tab and change the names of the physical files listed to a different name. If you are not using the “sa” login to connect to the database, you may need to change the database login.

To do this, launch Query Analyzer from SQL Server Management Studio. In the database you just restored, enter the following command:

SQL command "sp_change_users_login 'auto_fix' 'username'

Where: `username` is the username that jboss is using to communicate to the SQL Server.

MySQL

To restore MySQL databases, there are two methods.

To restore using the copied files restores all MySQL databases that were on the server at the time of the backup, not just the NA database. This method should only be used if NA is the only application using the database server.

1. Make a backup of the MySQL.
2. Stop the MySQL service (click My Computer --> Control Panel --> Administrative Tools --> Services).
3. Copy all of the files that were backed up from the `mysql\data` directory originally back into the `mysql\data` directory.
4. Restart the MySQL service.

To restore MySQL databases using the .sql backup file:

1. Make a backup of the MySQL database.
2. Edit the `.sql` file. Add the following line to the top of the file:
   ```
   SET FOREIGN_KEY_CHECKS=0;
   ```

   If you are restoring to a different database name, the foreign key constraints inside the dump file reference '<Database_Name>.RN_DEVICE' ('DeviceID'), including the database name. If you restore this to a different database name, in effect you are referencing the database <Database_Name> for your FOREIGN_KEY checks. This is a bug in mysqldump and how it interacts with the InnoDB table types. The solution is to remove the "<Database_Name>."

3. Navigate to the mysql\bin directory and enter the following command to get to the mysql command interface:
   ```
   mysql -h <hostname> -u <username> -p <password>
   ```
4. Enter the following commands in the mysql command interface. (Note that mysql needs forward slashes '/' in path names.)
   ```
   drop database <DatabaseName>;
   create database <DatabaseName>;
   use <DatabaseName>;
   source <BackupFileName>.sql;
   grant all privileges on <DatabaseName>.* TO <username> identified by
   '<password>';
   ```

   Where: `username` is the username that NA uses to connect to the database and `password` is the user's password.

   ```
   grant all privileges on <DatabaseName>.* TO <username>@localhost
   identified by '<password>';
   ```

   Where: `username` is the username that NA uses to connect to the database and `password` is the user's password.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click *here*.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **ovdoc-nsm@hp.com**.

Product name and version: NA 9.22.01

Document title: *NA Administration Guide, November 2014*

Feedback: