Release Notes

NRM 2.1

Network Resource Manager

Document Number: **NN48020-400**

Document Version: **03.02**

Date: **June 2009**

Copyright © 2004–2009 Nortel Networks, All Rights Reserved

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

Trademarks

Contents

Chapter 1
Getting started

Network Resource Manager (NRM) is an application that provides a suite of device management tools. You can use NRM to perform a variety of management tasks across multiple device types using a Web-based interface, including:

- distribution of configuration templates and scripts
- configuration backup and restore
- device password management
- inventory management
- log browsing
- task scheduling
- software version updates
- distribution of tunnelguard rules

About this guide

This guide is part of the NRM documentation suite and lists the release notes associated with the NRM 2.1.

Audience

This guide is intended for network engineers who use the Network Resource Manager to configure and maintain networks. This guide is based on the assumption that you have the following background:

- understanding of networking terminology, theories, and practices
- knowledge of the Windows operating system or Linux systems and graphical user interfaces (GUI)

Symbols and text conventions

These symbols highlight critical information for the NRM system:

Caution: Alerts you to conditions where you can damage the equipment.

Danger: Alerts you to conditions where you can get an electrical shock.

Warning: Alerts you to conditions where you can cause the system to fail or work improperly.

Tip: Alerts you to additional information that can help you perform a task.

Note: A Note alerts you to important information.

Security Note: Indicates a point of system security where a default should be changed, or where the administrator needs decide the level of security required for the system.

Warning: Alerts you to ground yourself with an antistatic grounding strap before performing the maintenance procedure.

Warning: Alerts you to remove the NRM main unit and the expansion unit power cords from the AC outlet before performing any maintenance procedure.

These text conventions are used in this guide to indicate the information described:

Convention	Description
`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`info`** command. Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.
italic text	Indicates book titles

Convention	Description
`plain Courier text`	Indicates command syntax and system output (for example, prompts and system messages). Example: `Set Trap Monitor Filters`
angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: <*InstallDir*>\database\tftp
braces ({ })	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **setAccess** {**o**|**g**|**w**}, you must enter **setAccess o**, **setAccess g**, or **setAccess w**.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **echo** [**-nonewline**], you can enter either **echo** or **echo -nonewline**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is **which** [<*command_name*>]**...** , you enter **which** and as many command names as needed.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **spawn telnet** <*ip_address*> , you enter **spawn telnet 192.48.33.7**.
separator (>)	Shows menu paths. Example: Choose View > Sort > by Name.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is **array *NewArray* =** [<*reference*> **|** <*referenceList*>] you enter either **array NewArray =** <*reference*> or **array NewArray =** <*referenceList*>, but not both.

Related publications

For more information about using NRM, refer to the following publications:

- *NRM Fundamentals (NN48020-300)*
- *NRM Installation Guide (NN48020-307)*

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

http://www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you don’t find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

http://www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

http://www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Chapter 2
Network Resource Manager

This guide lists the release notes associated with the NRM 2.1.

This chapter provides the following information:

Operational notes

This section provides operational notes for the Network Resource Manager 2.1 release.

NRM 2.1 migrates data from NRM 2.0 and NRM 2.0.1

If you have NRM 2.0 or 2.0.1 installed, the NRM 2.1 installer detects the earlier version and asks whether you want to migrate data from that version. If you choose to do a migration, a CMD window appears and prompts you to enter the administrator password. After you enter the password, the installer performs a common services backup. Record the name of the backup archive created.

When the common services archive is successfully created, you must close the CMD window. The migration proceeds to uninstall the previous version of NRM and installs NRM 2.1.

When the NRM 2.1 installation is complete, you are asked to decide whether you want to restore the archive that contains the data of the previous NRM version. If you select Yes, a CMD window appears; provide the archive name, the administrator password, and the module to be restored.

For more information about NRM installation, see *NRM Installation* (NN48020-307).

Operations not correctly propagated when user is simultaneously logged in to multiple browsers

In the event that the same user is logged in to NRM 2.1 concurrently through more than one browser, some operations are not correctly propagated between the browsers. Deleting a portlet in one browser, for example, may not be propagated to the other browser.

Recommended limits for executing tasks

A single NRM task is capable of performing operations against up to 10 devices at a time. Password changes, configuration backups, or software updates are examples of operations. As soon as the 10th device within a task is finished, the NRM will begin performing operations on the 11th device. If another task is launched while the first is still running, then operations against up to 10 additional concurrent and devices will be performed. Nortel recommends that you do not launch more than two or three tasks at the same time, so that you do not perform operations against more than 20 to 30 devices at the same time.

Devices associated with mulitple tasks

Note that if more than one task contains the same devices, NRM will run the operations only on the first task that gets activated. NRM supports inter-tool device locking, so once one tool locks the device, the other tools will skip that device as if it were not found in the inventory and log an error.

Disable Enhanced Security mode in Internet Explorer 7

If you are using Internet Exporer 7 (IE7) to access NRM, you must disable the Enhanced Security mode in in IE7. Follow the steps below to disable Enhanced Security.

1 Select **Control Panel > Add/Remove Programs**.

2 Select **Add/Remove Windows Components**.

3 Click the checkbox next to **Internet Explorer Enhanced Security Configuration**.

4 Click **Finish**.

Instructions for installing Network Resource Manager on Linux

Insert the CD into a CD/DVD drive, mount the drive. Open a terminal and copy NRM2.1.0.0_018.bin from the CD, to a local hard drive . Change the permissions of the file to allow execution (chmod 777). Run the file and follow the install instructions. For more information about installation, see *NRM Installation* (NN48020-307).

Instructions for installing Network Resource Manager on Windows

Insert the CD into a CD/DVD drive, if autorun does not launch the installer, select the file NRM2.1.0.0_018.exe and run it manually. Follow the install instructions. For more information about installation, see *NRM Installation* (NN48020-307).

Limitations

The following table lists limitations for the Network Resource Manager 2.1 release.

Table 1 Limitations

CR Number	Description
Q01909110	When using IE to view maximized portlets, the Properties Table displays poorly when you transition between the portlets using the tab key.
Q01914274	When the same user is logged in to two browsers, and deletes a portlet, the change is not propagated to both.
Q01923985	When you move portlets on the interface, the new position does not persist at relogin/refresh.
Q01930798	Memory leaks occur in IE for portlet creation, task creation, and editing.
Q02004639	When you add or remove columns from portlets in Firefox, the check boxes for selecting columns become blurred. In addition, an internet connection is required to properly display icons.
Q02007693	The migration from 2.0 or 2.0.1 to 2.1 must be done manufally if the releases are installed in different directories.
Q02011720	While a task is running on 30 devices, and you add a task or log filter, focus is lost.
Q02015455	Whea n session expires in a Firefox client on Linux, the browser may flicker intermittently.
Q02017783	If portlet is up with an activated task, the browser focus will remain on the portlet.
Q02019776	The Smart Diff JNLP download asks for user input two times before downloading the application.
Q02027951	An error message displays after clicking ok to the license pop up (intermittent).
Q02030639	Reinstalling NRM on a server with EPM/VPFM preserves NRM data on 2008.

Chapter 3
UCM Common Services

This guide lists the release notes associated with the UCM Common Services.

This chapter provides the following information:

Operational notes

This section provides operational notes for the UCM Common Services. It provides information on the following topics:

Installation

- English is the only language supported.
- Installation locations of the product and common services are greyed out. They can only be changed by clicking the 'Choose' button.
- If MySQL is already existing in the system and running, it needs to be stopped so that the Nortel UCM MySQL can be installed.
- Ports in the 1-1023 range (other than 80 and 443 for HTTP/HTTPS) should not be used. These are TCP/UDP ports that are used by a variety of applications : FTP (20,21), Telnet 23, SNMP 161 and so on. Choosing them may result in applications not working and other conflicts.
- Information about type of server:

— Primary Security Server - Security Administration is installed.

— Member Security Server - Security Administration not installed, redirected to primary server.

- — Backup Security Server - Takes over the function of primary in case of primary server failure.
- — Central Server - Device Credentials and License Module are installed.

- Check the host file entries on Linux (/etc/hosts) and Windows (C:\Windows\System32\Drivers\etc\hosts). Correct format of Fully-Qualified Domain Name (FQDN):

  127.0.0.1 localhost
  102.54.94.97 rhino.acme.com rhino

  Note: The value of FQDN mapped in hosts file will appear as default on Windows, and if it is DNS resolvable, also on Linux. Otherwise, the FQDN will have to be inserted manually. When multiple networks interfaces are active, the FQDN must be inserted manually. An eventual default value is not guaranteed to be the desired one. In member or backup mode installation, the hosts file should have entry for primary server. In non-central mode installation, the hosts file should have entry for central server.
- Add the server IPs(primary/member/backup) to hosts file on Linux (/etc/hosts) and Windows (C:\Windows\System32\Drivers\etc\hosts).
- High availability is not supported for Device Credentials and Licensing modules. Single Sign-on supports high availability. If a server having Device Credentials and Licensing modules is down/uninstaller/removed all other nodes refering to the server will not have access to Device Credentials and Licensing modules.
- If a primary server is restarted backup and member servers also need to be restarted. Order of restart should be primary, backup, member.
- On IE7 after login if you see a blank page https://your-fqdn.com/securityserver/UI/blank . Got to Tools > Security > Click "Restore all zones to default level"
- FQDN needs to have minimum 2 dots.
- When pointing to a CS1k as primary:

  a) The first product (EPM,NRM/VPFM/IPFM) pointing to CS1k primary needs to be a member. If its absolutely necessary to install the product in backup mode the destination xml files under JBOSS_HOMEserver\default\deploy-hasingleton\jms\clusteredDestinations need to be copied manually to the primary

  b) Q02038117 : If there was/is any product(EPM,NRM/VPFM/IPFM) using CS1k as primary the CS1k jboss needs to be restarted before installing the new product.

Security

- The default SSO token timeout is 120 minutes, regardless of whether there are user activities or not on a session. Additionally, The default idle timeout is 30 minutes, this is affected by user activities.

- The Active Session list in quantum administration page will list all the sessions that are not logged out and are within the application timeout limit.
- Application certificate is the server-side certificate created at installation time and there is 'client.truststore' file corresponding to it (for client-side calls) in the UCM installation folder. At any time users should not change the application's default certificate. Trying to change the application certificate might break some of the security functionalities. (Q01917319)
- IE7 will warn about the Certificate as the product certificate is not verified by the third party certificate authority(CA). User can avoid this warning by changing the IE setting in the advanced tab(Q01921773).
- Firefox issue: Some times we see a error in firefox "Your certificate contains the same serial number as another certificate issued by the certificate authority. Please get a new certificate containing a unique serial number. (Error code: sec_error_reused_issuer_and_serial)" This happens when the browser is not clearing the cached certificates. Closing the browser might not help. Kill the firefox process and restart the browser. To get the process id "ps -ef | grep firefox" .
- Registration of member/backup to primary is automated. But deregistration after a member/ backup is uninstall is manual. User need to remove the uninstalled member/backup from the elements table via the Security Administration screens.
- When using localhost or IP address in the browser address bar to access UCM page, user will be taken to a login page with a link 'Go to central login for Single Sign-On', clicking the link will switch the url in the address bar to FQDN. Note: Always use FQDN to access UCM page, single-sign-on is only supported on FQDN.

Backup and restore

- Backup and restore can only be run by users in 'Administrators' group (in Windows) or 'root' group (in Linux).
- Stopping backup or restore in the middle of the process (for example by pressing Ctrl-C) is not a supported scenario. The database and system state wont be guaranteed to be stable if this is done. To reduce possibility of users doing this, a warning message will be displayed at the beginning of backup and restore process.
- Restore of users and roles is not supported.
- Restoring will only append the backed up data to the database. Any updates/changes between Backup Restore operation will remain.
- Restoring Device Credentials will replace existing data.

Device and server credentials

- Spaces are not allowed in the device credential ranges.

License

- A known drawback of MacroVision license is that for the Linux platform the user can only use the MAC address associated with the eth0 interface of the server. MAC addresses associated with any other interface would deem the application unlicensed.

- Q02038117 : Export functionality: Selecting multiple rows of same product name might cause unexpected error. By selecting a product row, application exports all the licenses of the product name on all the connected UCM hosts(primary/member/backup).

User interface

- The login warning banner contains "[company name]" instead of a value.To modify it, go to Security Administration -> Security -> Policies. Then click on "Edit" for Security Settings. See ECC-318

Known issues

The following table lists the known issues and workarounds for UCM Common Services.

Table 2 Known issues and workarounds

Issue	**Description**
IPv6	Problem observed when starting JBoss on Linux. At startup, JBoss is trying to bind an IPv6 IP and it fails. The result is that JBoss is not correctly started. This is happening due to a known bug from JDK 1.5 that was solved in JDK 6. Here is the JIRA issue for this problem: http://jira.jboss.com/jira/browse/JGRP-47 **Workaround:** Add the following option in JBoss startup script (until the switch to JDK 1.6): Djava.net.preferIPv4Stack=true See the JBoss wiki for more information about this issue, at the following location: http://wiki.jboss.org/wiki/IPv6 This issue and workaround only apply to hybrid boxes (having both IPv4 and IPv6 support). There is no workaround for pure IPv6 boxes.

Limitations

The following table lists the limitations for UCM Common Services.

Table 3 Limitations

CR Number	**Description**
Q02038860	Cannot add a IPv6 Address Range in Device and Server Credentials.