



NetMRI 7.2.1 Release Notes

TABLE OF CONTENTS

INTRODUCTION 2

 About NetMRI 7.2.x 2

NEW FEATURES 2

 NetMRI 7.2.1..... 2

Deprecated and Obsolete features 3

DEVICE SUPPORT UPDATES 4

 LIMITATIONS OF 7.1.x SOFTWARE 5

UPGRADE GUIDELINES 5

 Special Notes on Upgrading From pre-7.0.1 Releases..... 6

 Upgrading From 7.0.x..... 6

 Special Note on External Authentication/ Authorization Services..... 6

 Upgrade Sandbox Instances..... 6

OTHER REQUIREMENTS 6

 Tested Browser Versions 6

 Supported VMware Versions 7

TECHNICAL SUPPORT 7

RESOLVED ISSUES 8

 Fixed in NetMRI Release 7.2.1 Documentation..... 8

 Fixed in NetMRI Release 7.2.1 8

KNOWN ISSUES FOR NETMRI RELEASE 7.2.1 11



NetMRI 7.2.1 Release Notes

INTRODUCTION

This release note needs to start with a quick note of explanation. The process of reverting the name back to NetMRI is complete except for the name of the build.

All existing customers have the option to upgrade their deployments to auto-failover configuration for both standalone, Operations Center and collector appliances.

About NetMRI 7.2.x

Upgrading to 7.2.1 must first go through an upgrade to 7.0.x (7.0.5 is recommended). Customers running NetMRI 6.9.x, or earlier releases are encouraged to upgrade their systems to 7.0.x and must refer to the 7.0.5 release notes. Pay special attention to the upgrade guidelines and review all feature changes as there are numerous considerations that must be taken into account.

Since NetMRI 7.1.1 active penetration scanning is conducted. This is in addition to the vulnerability scans conducted on previous releases. All reported and discovered SQL injection vulnerabilities have been fixed. A number of other vulnerabilities have been found and fixed as well, but the work for the lower severity vulnerabilities is not quite complete and will be addressed in the upcoming releases. All vulnerabilities require an authenticated user to initiate the action. No un-authenticated exploits exist to the limits of our testing ability.

The following sections describe the 7.2.1 feature set improvements, additional device support, upgrade guidelines, resolved issues, and known issues.

NEW FEATURES

This section describes new features for this release.

NetMRI 7.2.1

Support for Cisco ACI Discovery

NetMRI 7.2.1 introduces the support for Cisco ACI. With this feature, NetMRI connects to the ACI controller using the REST interface, retrieves SDN overlay objects such as Tenants, Bridge Domains, Application Profiles, and End Point Groups; as well as traditional underlay objects such as VLAN, VRF, and Interfaces and connected endpoints. Each spine and leaf node is processed as a separate managed device. To discover the data from the controller, you must provide the http(s) credentials.

Support for Aruba and Cisco Wireless Controllers and Access Points

This feature enables the support for Cisco and Aruba Wireless Controllers and thin Access Points. Information on the end-hosts connected to the access points is presented under the Switch Port Management. Additional data has been added: AP name, AP IP and SSID.

Python Scripting

It is now possible to run Python scripts from the NetMRI Job engine. The version of the Python interpreter installed on the sandbox (where the scripts are run) is 3.4.3. The Python client API can be downloaded from the NetMRI appliance if running Python scripts external to the NetMRI appliance is desired.

User Generated License

Starting with 7.2.1, users can generate their own NetMRI licenses for the appliances without involving the Infoblox team. This allows for easier management of the collector licenses when the number of devices varies with time on the collectors. New audit logs have been added to allow the Infoblox team to ensure that there is no misuse of the feature.



NetMRI 7.2.1 Release Notes

Additional Changes for 7.2.1 Release

Existing customers will see the following changes in their NetMRI deployment after upgrading to Release 7.2.1:

- IPAM Sync Enhancements:
 - Additional wireless discovery data is now included with the end point IP addresses being synchronized with NIOS. The additional data includes wireless access point name, wireless access point IP address and SSID. This complements the wireless controller that was already being synchronized. The compatible NIOS version is 8.3.
 - If discovering Cisco ACI environments, additional discovery data is now included with IP addresses and networks being synchronized with NIOS. The additional data includes tenant, EPG, and bridge domain. The compatible NIOS version is 8.2.
- A searching capability has been added to the **Add-Rules-to-Policy** selector under **Config Management -> Policy Design Center -> Policies**.

Deprecated and Obsolete features

This section describes features no longer supported in this release, or planned for removal in a future release. These features are ones that have not been adopted by customers, or were for specific cases in the past. Since NetMRI contains such a rich feature set, these items are being trimmed to ensure that the focus can be placed on improving those features that are in use, and adding new features in areas where use cases are growing.

Deprecated Features

Deprecated features are features that are skipped during release qualification. The code remains unchanged, but may be removed in a future release.

There are no deprecated features in NetMRI 7.1.x. Please refer to the 7.0.5 Release notes for the list of the deprecated features in the 7.0.x version train.

Obsolete Features

The following existing features were deprecated in 7.0.x and are now obsolete in 7.1.1. Testing of these features was skipped during release qualification. Functionality and screens may be removed as of this release. Customer cases resulting from bugs found in these features will not be acted upon, excepting significant circumstances.

- Remote Diagnostic Tool
- Cisco Call Manager
- Quality of Service test module
- VoIP SLA test module

Planning for Deprecated and Obsolete Features

The following features are candidates for becoming deprecated or obsolete in a subsequent release.

- Standard + SPM license combination - replaced by 'Full NetMRI' license type
- TAE Module
- HTTP connections - limiting the system to HTTPS only



NetMRI 7.2.1 Release Notes

DEVICE SUPPORT UPDATES

The following devices are newly support or updated for Release 7.2.1:

- Alcatel OS6450C48, s/w ver 6.6.4.244.R01 GA, Switch-Router
- Avaya G450, ver 36.17.0, Media Gateway
- Avaya G430, ver 36.16.0, Media Gateway
- Brocade vRouter 5415, Version VSE6.7R10, Router
- Brocade ICX6450-48-HPOE, version 07.4.00fT311, Switch
- Brocade ICX6610-24F, IronWare Version 07.4.00fT7f1, Switch
- Cisco cat6509, ver 12.2(33)SXH4, Switch-Router
- Cisco cat3560x48, version 12.2(58)SE2, Switch
- Cisco cat3560x48P, version 12.2(58)SE2, Switch
- Cisco CatWSC3560CX12pcS, ver IOS 15.2(3)E1, Switch
- Cisco C385024S, ver IOS-XE 03.07.01.E, Switch
- Cisco ASR1006, ver 15.4(3)S4, Router
- Cisco N5kC5596Up, Ver 5.2(1)N1(7), Switch
- Cisco N9Kc9504, ver 7.0(3)I4(5), Switch-Router
- Cisco ASR9010, ver IOS-XR 5.3.3[Default] and IOS-XR 5.1.3[Default] , Router
- Cisco MEC6524gt8s, ver 12.2(33)SX17, Switch-Router
- Cisco catalyst295048T, ver 12.1(22)EA4a, Switch
- Cisco N7Kc7010, ver 7.2(0)D1(1), Switch-Router
- Cisco N9Kc9396PX, ver 6.1(2)I3(4b), Switch-Router
- Cisco ASR 1006, v15.5(3)S4a, Router
- Cisco 2911, v15.2(4)M9, Router
- F5 Viprion-B2250, ver 12.1.2, Load Balancer
- Force10 s4810, ver 9.11(0.0P4), Switch-Router
- Fortigate fgt1240B, ver 5.0.10, Firewall
- Fortigate fgt3950B, v5.0.10, Firewall
- H3C 513048GPoEPlus4SFPPlus370WEI, ver 7.1.045, Release 3115P05, Switch-Router
- H3C s7510E, v5.20, Switch-Router
- H3C 10512, ver 7.1.070, Release 7523P03, Switch-Router
- H3C 10504, ver 5.20, Release 1201, Switch-Router
- HP VCFlex-10-10D-Module, v4.20, Switch
- HP VCEthernetModule, v3.30, Switch



NetMRI 7.2.1 Release Notes

- HP ProCurve J9280A, s/w ver Y.11.47, Switch
- Huawei s5700-28TP-LI-AC, ver V200R006C00SPC500, Switch-Router
- Ibmnetwork EN4093, ver 7.8.10, Switch
- Juniper EX3200, ver 14.1X53-D40.8, Switch-Router
- Juniper EX8208, v12.3R12.4, Switch-Router
- Nortel VSP4850GTS, ver 5.1.1.4, Switch-Router
- McAfee WBG-5500C, ver 7.6.2.6.0 Web Gateway

LIMITATIONS OF 7.1.x SOFTWARE

Device Group recalculations after Editing Device Group Criteria

When you change Device Group membership by changing the criteria for a group (for information, see [Understanding Device Group Membership Criteria](#) in the *Infoblox NetMRI Admin Guide*), the appliance recalculates group membership for the specified parent device group but does not automatically update or recalculate child groups and descendant groups until the standard periodic Device Group refresh cycle takes place. **WORKAROUND:** Use the Admin Shell CLI command **refreshgroups** to recalculate all device groups in the tree after changing the membership criteria.

Inbound TFTP/HTTP File Transfers from VRF-Aware Devices

NetMRI provides Config Template and Rollback features, in which the involved devices initiate the file transfer connections. Due to the adoption of Network Views in 6.9.x, a device that starts a connection to NetMRI needs to specify the interface it has present in the correct network view. However, this is not consistently possible on supported VRF-aware devices. **WORKAROUND:** TFTP/HTTP file transfers on VRF-aware devices will work when the NetMRI manages the device on the device's default VRF; when the device's Management IP address is on an interface in the device's default VRF (such as **(default)IOS** for Cisco IOS, **default** for Nexus and **master** for JunOS). If NetMRI cannot reach the VRF-aware device through the device's default VRF, this feature will not be available.

SNMP Credentials in Juniper VRFS

For discovery and periodic polling on Juniper devices through an interface that is not in the Juniper default VRF (master), the query must use a special "default@credential" format. This setting assumes that users do not have management interfaces in a VRF. Hence, the SNMP credentials for VRF-aware Juniper devices must use syntax similar to: "@vrfsnmp." Enter these values for SNMP credentials under Settings icon -> **Setup** -> **Credentials** -> **SNMP v1/v2c** tab. (When querying VRF-aware Juniper devices via an interface that is in the default VRF, a plain community string can be used without the "@" character.)

UPGRADE GUIDELINES

NetMRI 1102-A appliances do not support the 7.2.1 release and cannot be upgraded to 7.2.1.

NetMRI systems (standalone or Operation Center) can be upgraded to 7.2.1 starting from the following versions: 7.0.1 7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.1.1, 7.1.2, 7.1.3 and 7.1.4

The upgrade image file is `ib_network_automation-v 7.2.1.87960.gpg`.

Data collection is shut down on Operations Centers during the 7.2.1 upgrade. In Operations Center Controller-to-Collector communications, all collected network data passes from the Collector to the Controller through a tunnel connection. Tunnel connections are shut down during upgrades to 7.2.1.



NetMRI 7.2.1 Release Notes

Special Notes on Upgrading From pre-7.0.1 Releases

Upgrading from earlier versions must pass through an upgrade to 7.0.1 (7.0.5 is recommended). Customers must read and follow the upgrade instructions in the 7.0.5 Release Notes. Those instructions are not repeated here, but are still relevant in the upgrade process from the previous versions.

Upgrading From 7.0.x

You can directly apply the NetMRI 7.2.1 upgrade to systems running NetMRI 7.0.x.

For customers with systems that do not connect to the Internet/AutoUpdate server, you will need to download the upgrade image file and SCP it to the admin users' directory on the appliance. Then run the standard AutoUpdate utility from the NetMRI Admin Shell to perform the 7.2.1 upgrade.

Special Note on External Authentication/ Authorization Services

If using external authentication over SSL, ensure it supports TLS 1.2. prior to upgrading NetMRI.

Upgrade Sandbox Instances

Ensure that Sandboxes (either Local or Remote) are fully and properly upgraded (to the starting release version) prior to starting an upgrade. If the sandbox is in an incorrect state prior to a follow-on upgrade, this may create issues that are difficult to diagnose.

- Local sandbox instances for NetMRI will be automatically upgraded.
- Remote Sandbox instances (example: Sandbox instances on a VM server) must be manually upgraded using the 'sandbox reset' command from the admin shell. See the topics [Using the NetMRI Sandbox](#) and [Setting Up a Remote Sandbox](#) in the online Help for more information.

OTHER REQUIREMENTS

Tested Browser Versions

NetMRI 7.2.1 has been tested with the following Web browsers:

OS	Browser
Microsoft Windows 7®	Microsoft Internet Explorer® 11.x Mozilla Firefox 53.x Google Chrome Latest(Ex:60.x)
Microsoft Windows 8.1®	Microsoft Internet Explorer 11.x Mozilla Firefox 53.x Google Chrome Latest(Ex:60.x)
Microsoft Windows 10	Microsoft Internet Explorer 11.x Mozilla Firefox 53.x Google Chrome Latest(Ex:60.x)
Apple® Mac OS X 10.12.5	Safari 10.x

The unsupported browser warning has been removed. There may be occasional display issues as these browsers go through their rapid release cycle; however, we expect enough compatibility in their coding that it doesn't make sense to highlight the version difference in red during every login.



NetMRI 7.2.1 Release Notes

When viewing NetMRI, set the screen resolution of your monitor as follows:

Minimum resolution: 1024x768

Recommended resolution: 1280x800 or better

Supported VMware Versions

Infoblox offers NetMRI in a virtual machine version. The following VMware releases support NetMRI 7.1.4 VM operation:

- ESXi 5.0x and ESXi 5.1x
- VMware Workstation 10.1
- Fusion 7.1 on Mac OSX 10.9 (NetMRI Standalone mode only)

TECHNICAL SUPPORT

Product Support

Infoblox technical support contact information:

Telephone: 1-888-463-6259 (toll-free, U.S. and Canada); EMEA, +32 3 2590440; +1-408-986-4000, ext. 1

E-mail: support@infoblox.com

Web: <https://support.infoblox.com>

Documentation

Download the latest documentation from the Infoblox Support page: <https://support.infoblox.com/app/docs>.

Training

Training information is available at: <https://training.infoblox.com>.



NetMRI 7.2.1 Release Notes

RESOLVED ISSUES

The following issues were reported in previous NetMRI releases and resolved in this Release.

Fixed in NetMRI Release 7.2.1 Documentation

NETMRI-29183 - Update documentation on the set of characters allowed in the PRINT command

NETMRI-29100 - Document the Disable HA feature

Fixed in NetMRI Release 7.2.1

NETMRI-29093 - Waiting on consolidator dependency for one Collector stops other Collectors

NETMRI-29068 - Log4perl causes log files to be opened multiple times

NETMRI-29058 - Add logging of device license add/delete

NETMRI-29057 - Add Message Timestamp to scriptxml logs

NETMRI-29055 - Additions to Discovery Diag output for 7.2.1

NETMRI-29054 - "Vlan Interface Summary" report failing to collect data.

NETMRI-29033 - Shell injection possible when setting admin password with special characters

NETMRI-29030 - Need to limit VDC (virtual device context) type recognition only for Cisco Nexus 7000 and 3000 platform

NETMRI-29000 - License install broken

NETMRI-28990 - OC: Policy consolidator: 'too many open files' and subscriptions not processing right

NETMRI-28981 - OC: volatile Device Properties are not updated if nothing else changed

NETMRI-28979 - IPAM Sync Failure - tables too big for memory

NETMRI-28941 - Report output exceeding 1024 character of width in a line are truncated

NETMRI-28937 - Update server.xml when changing eth0 interface IP Address via the GUI

NETMRI-28929 - Address Force10 vendor's SwitchPort data collections issues

NETMRI-28900 - Recognize Admin VDC for Cisco Nexus and adjust collection datasets

NETMRI-28893 - Assigning >51 device groups to a remote user role assigned causes login problems

NETMRI-28883 - Anomaly when exporting configs

NETMRI-28862 - Deleted devices still generate consolidator changes

NETMRI-28857 - InnoDB tables in consolidator import_history leaves behind orphaned sql files

NETMRI-28856 - Discovery tables in netmri database not cleared when device is deleted

NETMRI-28841 - Add errorIgnore for "%Error opening bootflash:crashinfo (File not found)"

NETMRI-28830 - A device with a blank MAC Address can end up as an SPM End Host without a MAC Address

NETMRI-28810 - Config compare page does not show all the lines in IE

NETMRI-28778 - Add default vrf option for config template bulk mode of Cisco NX-OS

NETMRI-28775 - Device MAC is removed if ARP entry goes away

NETMRI-28771 - Add setting of SSH MAC algorithm to Admin CLI Configure command



NetMRI 7.2.1 Release Notes

- NETMRI-28762** - Custom field with UTF-8 data does not display properly in the GUI
- NETMRI-28761** - Curl API update fails with UTF-8 data
- NETMRI-28739** - summary system alert notification breaks on attempt get cleared issue details
- NETMRI-28736** - Add Port control feature support for Nortel VSP4850GTS 5.1.1.4 Switch-Router
- NETMRI-28732** - API: spm grids do not honor 'select'
- NETMRI-28721** - Using GroupID as array index causes index error
- NETMRI-28709** - SwitchPort data collection needs to be part of forwarding data collection when forwarding data collection is done via CLI
- NETMRI-28704** - Fix rails undefined local variable in discovery_settings_controller.rb
- NETMRI-28695** - Collect device Model name and Inventory info for Brocade vRouter devices using CLI
- NETMRI-28671** - Fix handling of values with double quotes in CCS_Engine.pm
- NETMRI-28655** - Shell injection in License script
- NETMRI-28652** - CPD rule fails to evaluate due to 'End' statement in the middle of configuration file
- NETMRI-28637** - Enrich issueCleared Events with Issue details. Revert previously added in 7.1.3 changes as they don't take effect for e-mail notifications.
- NETMRI-28628** - Suppress errors during VRF data collection for Cisco Admin Context
- NETMRI-28618** - CPD rule fails with error "Invalid Indent On Line"
- NETMRI-28597** - DSB sync is failing due to shell injection in settingsd
- NETMRI-28592** - (Some) H3C devices have random CRLF (or its parts x0D x0A) chars which creates fake config diffs
- NETMRI-28591** - Vlan consolidator ignores some of Juniper interfaces
- NETMRI-28555** - UI: Audit log reveals changed user's password in clear text
- NETMRI-28525** - Add port channel support for Cisco Nexus N5K, N6K, N7K and N77 devices
- NETMRI-28524** - Network Explorer > Discovery table Improve sorting criteria for ConfigCollection field
- NETMRI-28482** - Add config collection update for SEL Console Server devices
- NETMRI-28476** - Add timestamp to show tunserver/tunclient output
- NETMRI-28471** - Implement model/version filter for SNMP Vlan collection to restrict unneeded collection for affected devices
- NETMRI-28463** - Adding Wireless data collection support
- NETMRI-28404** - Prevent user from configuring eth0 interface with IP Address 169.254.1.1
- NETMRI-28337** - Adding VRF support for Cisco IOS-XR
- NETMRI-28290** - (Some) HP devices are outputting terminal control characters to the job output
- NETMRI-28274** - Support config template bulk mode for Cisco NX-OS
- NETMRI-28182** - Add correct trunk support for HP ProCurve J9280A model
- NETMRI-28144** - Add vlan data collection support for F5 Load Balancers and fixing typo in SNMPVlanCollection.sql for F5
- NETMRI-28099** - Support tools need to be updated to work with failover



NetMRI 7.2.1 Release Notes

NETMRI-27767 - Reports: poor handling of excessively large scheduled reports

NETMRI-27616 - Policies: "Enforce This Rule" does not reflect checks deletion properly

NETMRI-26794 - Double quotes (") are double escaped in CCS input

NETMRI-22570 - Cannot select all interfaces on a device or for device group when creating a report on Interface History data



NetMRI 7.2.1 Release Notes

KNOWN ISSUES FOR NETMRI RELEASE 7.2.1

The following items are notable bugs or potential improvements found by Infoblox, or reported by customers. These are candidates for future maintenance or major releases. For information on specific tickets, please contact support.

- NETMRI-29241** - Link to the device list is still pointing to the 7.1.4 list. Updated list can be found on the portal
- NETMRI-29035** - VLAN information is not displayed for endpoints connected to wireless access points
- NETMRI-29015** - VRF name is not displayed for interfaces of Cisco ACI leaf switches that are assigned to EPG but are not connected to end hosts.
- NETMRI-28906** - Schedule archive does not differentiate between every day and every weekday.
- NETMRI-28226** - 2200 units stuck on starting network service. Manual reboot necessary.
- NETMRI-28192** - OC: Backpressure stream goes missing for unknown reason
- NETMRI-28123** - PruneData of netmri.SNMPGuesser and report.DevicePasswordLog does not work
- NETMRI-28070** - Archive reports success even though database is corrupted
- NETMRI-28017** - SwitchPortObject overwhelmed when device returns too much data
- NETMRI-27994** - Re-running a restore after a failed restore fails
- NETMRI-27993** - Prevent archive from running during a restore
- NETMRI-27983** - Populate dsb_sync directory on OC startup
- NETMRI-27948** - Raise System Health Alert if PruneData is not able to complete
- NETMRI-27933** - Check and fix an invalid logrotate.status file during Weekly Maintenance
- NETMRI-27907** - Config collection times out on Cisco devices with CatOS due to bad prompt regexps
- NETMRI-27355** - Need a help topic context for Topology > Path Analysis
- NETMRI-27336** - ccs jobs fail to start every weekly reboot
- NETMRI-27212** - Assign NeighborID in SwitchFwd associateNeighbors when IP Address is learned
- NETMRI-27010** - After rebooting primary on G8, roles are switched
- NETMRI-26565** - Seed device keeps getting re-discovered even after getting de-duplicated repetitively by another seed device
- NETMRI-26386** - Prevent maintenance from being run manually when archive is running
- NETMRI-25100** - Add aggressive log pruning to PruneData when disk space gets dangerously low
- NETMRI-25081** - Delete related job_targets entries without a job_specification entry
- NETMRI-24906** - netmri.ifGroupIssueSettings is not populated on Collector
- NETMRI-24856** - OC: Actively Confirm/Fix Collector Scan Interfaces entries
- NETMRI-24004** - remove global variables from dataEngine/common.pm
- NETMRI-23907** - nexthop of ipv6 ::1 is not shown correctly in Device viewer route table
- NETMRI-23835** - optimize DetectedChange consolidation query/queries



NetMRI 7.2.1 Release Notes

NETMRI-23683 - when copying report.Device entries to netmri.Device for Device Viewer on OC, update the DeviceID on duplicate

NETMRI-23435 - Sync timezone/ntp server settings to local sandbox.

NETMRI-23037 - Credential Collector triggers oom-killer after failed 6.9.1 upgrade

NETMRI-22902 - update tzdata to account for new updates

NETMRI-22527 - Exporting a built-in HTML report to PDF where the content is divided into multiple pages, the PDF retains the HTML page numbering

NETMRI-21232 - oc_proxy is not properly determining the effective user

NETMRI-20739 - Collector swapped out continues to send backpressure messages to OC

NETMRI-20682 - Device Group Counts in GUI may be incorrect due to Devices expiring or being rediscovered

NETMRI-20033 - DetectedChange/ChangeTrace does not properly consolidate over a month boundary

NETMRI-19796 - when determining a device type in getDeviceTypeProps.sql, only consider HSRP if it is for the same DeviceID

NETMRI-19706 - Remote Sandbox displays 'Net-SNMP' as Vendor under NetMRI

NETMRI-19687 - Wrap sql table upgrades in perl script to better catch errors and handle Lost Connection gracefully

NETMRI-17802 - Lock CVS repository during archive

NETMRI-17798 - Ensure updating DNS Servers updates Sandbox /etc/resolv.conf

[End of Document]