Dell EMC OpenManage Network Manager v.6.5.3

Release Notes

October 8, 2018-5 Rev. A01

Release Type and Definition

Numbers in parentheses below refer to issue tracking numbers.

Version:

6.5.3

Release Notes Date:

October 8, 2018

Upgrade Path Matrix

Rel Version	6.0SP1	6.0SP2	6.0SP3	6.1	6.1SP1	6.2	6.2SP1	6.2SP2	6.2SP3	6.5	6.5.2	6.5.3
6.0SP1	NA	x	x	NS	NS	NS	NS	NS	NS	NS	NS	NS
6.0SP2		NA	x	x	NS	NS	NS	NS	NS	NS	NS	NS
6.0SP3			NA	x	x	NS	NS	NS	NS	NS	NS	NS
6.1				NA	x	x	NS	NS	NS	NS	NS	NS
6.1SP1					NA	x	x	NS	NS	NS	NS	NS
6.2						NA	x	x	NS	NS	NS	NS
6.2SP1							NA	x	x	NS	NS	NS
6.2SP2								NA	x	x	NS	NS
6.2SP3									NA	x	x	NS
6.5										NA	x	x
6.5.2											NA	x
6.5.3												NA

New Features/Devices Supported in 6.5.3

OS 9

- Support FTOS 9.14.0 for existing models (S30XX, S31XX, S40XX, S48XX (S4810, S4820T and S5048F will be supported when 9.14.1 is supported in OMNM), S60XX, S61XX, Z91XX, MXL,MIOA, FNIOM) (30571)
- OS 9 - FTOS or OS10 switches don't provide relevant information in MIBs, so as a result fans/power supply alerts will not correlate to the appropriate component.(30975)
- Mac address may show incorrect value for S6010 and S4248FB (31266)
- C9010 not populating service tag at card level (HD-37717)

OS 10

- OS10 does not support SNMP v3 CLI commands (31348)
- OS10 no longer receiving "Availability: partial results" for default interface monitor (30704)
- OS10 device's firmware currently does not support CPU and Memory information. (30668)
- OS 10.4.1 does not support QBridge and Bridge mibs. As a result VLAN, Port switch mode and duplex information are not provided in OMNM (31046, 31031)
- OS 10.4.1 - no warmstart trap seen (31312)
- OS 10.4.1 - no coldstart trap seen (31311)
- OS 10.4.1 The lldpRemTable (from the LLDP-MIB) of a Dell OS 10 device cannot currently be viewed through the Mib Browser (31324)
- OS 10.4.1 is now supported on 3048-ON, S4048-ON, S4048T-ON, S6010-ON, Z9100-ON, S4128F-ON, S4148F-ON, S4128T-ON, S4148T-ON, S4148U-ON, S4148FE-ON, S4248FB-ON, S4248FBL-ON, S5148F-ON, and Z9264F-ON (PV-30518, PV-30526)
- OS10 - A configuration change trap may not be emitted from the device after a configuration change (31361)
- OS10 - The speed of the port will show when the port has an ethernet link connected to the switch, otherwise, the port speed will be showing as 0 (30737)

OS 6

- Support has been added for OS 6.5.2 for existing N-series models and these new models N3024ET-ON, N3024EP-ON, N3024EF-ON, N3048T-ON (30519)
- The OMNM 6.5.3 release supports a new feature for Dell N-Series CPLD updates for OS 6.5.2. This feature requires an updated license. You may request the license by sending an e-mail to sales@dell-omnm.com. (HD-37687)
- The OS 6 N-series switches don't provide relevant information in MIBs, as a result, fans/power supply alerts will not correlate to appropriate component.(30975)

Other Device Model Addtions

- Support added for Cisco ISR 4400, ISR 4300 (HD-38526)
- Support added for Fortinet Full SNMP_CLI driver (30483)

- Cisco support has been added for WS-C3650-24PD-S and WS-C3650-48PD-S (HD-38418)

Integration

- A REST API has been added to support programmatic firmware Deployment (31105)

Enhancements:

- "The Virtual Appliance menu option 4 has been changed from 4) Configuration Review" to "4) Generate Technical Support Logs File" This option will now auto-create the necessary log file for submission to support.

Other Known Issues

- Device warranty information returning mismatch between the actual warranty and contract info - If the Dell Warranty database has 2 records in their database that are essentially for the same product/service but they have different start and end dates, you may receive false alarm when one expires falsely indicating a warranty has expired. In reality there can be another contract covering the product or service. If you suspect a faulty alarm please confirm using the Dell online warranty information to confirm. In OMNM you may review warranty info on the device's detail page under the maintenance information that should correlate to each other, OMNM does not know how to do this correlation. (HD-38506)
- Due to limited MIB support in OS 10.4.1.0.X.453, the S4148T will only have the management port and 4 Ethernet ports discovered when switch-port-profile is set to profile-1; the S4148T will only have the management port and 6 Ethernet ports discovered when switch-port-profile is set to other profile (profile-2, profile-3, profile-4, profile-5 or profile-6) (30735)
- Dell DNOS, FTOS or OS10 switches don't provide relevant information in MIBs, so as a result fans/power supply alerts will not correlate to appropriate component.(30975)
- When accessing the Equipment's Alarm details page and choosing Equipment details, the data may not be displayed. You may go directly to the general tab instead to see equipment details (31536)
- When accessing some right-click menu option from the Resource Manager on the home, the pop screen may be rendered off-screen. As a workaround, before the operation, you can use crtl "-" to reduce the browser size and bring the pop up into view. (31539)

Resolved Defects

- C9010 is know populating service tag at card level (HD-37717)

New Features/Devices Supported in 6.5.2

- Driver support added for PCT and N3048EP, models on OS 6.5.1. (30557)
- Driver support added for the S5048F model on OS 9.12.1. (30122)
- Driver support added for QFX 10008 to the Juniper driver. (hd-37430)
- Cisco Nexus OIDs were updated to include the following Nexus models: 2224TP, 2232PP, 2232TM, 2232TM-E, 2248PQ, 2248TP, 2248TP, 2248TP-E, 2248TP-E, 2332TQ, 2348TQ, 2348UPQ, 3048, 3132Q40GE, 3132Q40GEOE, 3132Q40GS, 3132Q40GX, 3132QV, 3132QVOE, 3132QXL40GX, 3132QXOE, 5548UP Switch, 5596UP Switch, 56128P Switch, 5672UP Switch, 5672UP Switch, 6001-64P Switch, 6001-64T Switch, 6004-96Q Switch, 9372PX Switch, 9372TX Switch, 9396PX Switch, 9396TX Switch, C3172PQ-10GE, C3172TQ-10GT, C93180YC-EX. (28940, 28108)
- Driver support was updated to include the following Enterasys models: C3K122-24, C3K122-24P, C3G124-48, V2H124-24, G3G124-24(P), G3G170-24, S4, X4, C5K175-24, A2H124-24/48(P), A4H124-24/48(P), B2H124-48(P), B3G124-24/48, B5G124-24/48, B5K125-24/48, D2G124-12(P), A4H254-8F8T. (hd-37431, 27303)
- OS10 device driver to support ONIE devices running OS10 firmware was added: S3048-ON, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148FE-ON, S4148T-ON. S4148U-ON. (29030)

  This device's firmware currently supports **only** temperature KPIs and does not return power supply or fans information. (30668, 30665)

  NOTE:

  While other models may be listed in the products device driver support page, the S3048-ON, S41XX-ON models are the only ones officially supported.
- Dell Support Assist Feature for OS10: The getting started portlet asks for information regarding the user Dell Account. The "State/Province/Region" field currently is set as not mandatory field, if this fields is not populated, the post discovery action to the configure Support Assist will fail at Device Discovery time. Discovery will be successful but support assist will not be configured on the target device(s). The work around is to populate the field and run the Support Assist action from the Actions portlet. (30847)
- S4112T model fails deployment when using telnet. (30793) Workaround: Use SSHv2 to deploy S4112T model.
- Due to OS10 firmware issues with the S4148T model, OMNM discovers only 4 ethernert ports. As a result, sflow and performance data collection does not work propertly in OMNM. (30735)
- S4148U: Null point exception during Device Discovery, Resync. The S4148U has partial support for the entity mib and may show errors at discovery time. After discovery the device may be missing port information. As a result the default Interface monitor cannot monitor these ports. Any port level configuration through Actions like the automated port level Traffic Flow configuration will not function due to lack of a target port. The will be resolve in the next release. (30884)
- N-series device now supports OS version 6.5.0 and 6.5.1. (30126, 30127)

  N1108P-ON, N1108T-ON, N1124P-ON, N1124T-ON, N1148P-ON, N1148T-ON, N1524, N1524P, N1548, N1548P, N2024, N2024P, N2048, N2048P, N2128PX-ON,

N3024, N3024F, N3024P, N3048, N3048-EP, N3048P, N3132PX, N4032, N4032F, N4064, N4064F

- Dell Force 10 devices now support OS 9.13. (30125)
- Seeded compliance policies were added for Powerconnect (PCT) and FTOS devices. (29352)
  - Dell Networking (PCT/FTOS) recommended NTP
  - Dell Networking (PCT/FTOS) recommended Radius
  - Dell Networking (PCT/FTOS) recommended DNS
  - Dell Networking (PCT/FTOS) recommended Hostname
  - Dell Networking (PCT/FTOS) recommended SNMP Communities
  - Dell Networking (PCT/FTOS) recommended SSH
  - Dell Networking (PCT/FTOS) recommended Support Assist
- The following seeded Dell FTOS/DNOS event processing rules were added: (29894)
  - Dell FTOS Syslog Security Messages
  - Dell FTOS User Login
  - Dell FTOS User Logout
  - Dell FTOS Login Failure
  - Dell FTOS Config Change
  - Dell DNOS User Login
  - Dell DNOS User Logout
  - Dell DNOS Login Failure
  - Dell DNOS Config Change
- S5048F - Service Tag is NA and updated only after Resync (30838)
- Linux servers discovered via WBEM or Windows servers via WMI may now have an associated ssh CLI management interface that supports Actions. (26869)
- The flash based topology screen now displays a message when flash is not properly configured. The message provides high-level steps on how to resolve for each of the supported browsers. (30543)
- Prior to 6.5.2, the trial was imported and the 30-day expiration banner was observed. Starting with 6.5.2, the trial license no longer impacts upgrade. (30539)
- You can now perform DNS Resolution Monitoring against WBEM enabled devices. (30062)
- You can now monitor the target URL HTTP status. (30057)

  On Linux devices (CentOs), the Perl Libraries HTTP::Tiny and IO::Socket::SSL will need to be installed to utilize the Get URL Status and Get URL Status of Device Actions as well as the URL Status of Device Monitor. It is suggested that the cpan command should be used to install the new libraries. (30057)
- You can now monitor the TCP port status. (30056)

- The MySQL database was upgraded to 5.7.19 to resolve the following vulnerabilities. (29919)

  MySQL CPU January 2017: CVE-2017-3312, CVE-2017-3258, CVE-2017-3244, CVE-2017-3238, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3291, CVE-2017-3265, CVE-2016-8318, CVE-2017-3273, CVE-2017-3257, CVE-2016-8327, CVE-2017-3243, CVE-2017-3256, CVE-2017-3251, CVE-2017-3319, CVE-2017-3320

  MySQL CPU April 2017: CVE-2017-3308, CVE-2017-3309, CVE-2017-3329, CVE-2017-3453, CVE-2017-3456, CVE-2017-3461, CVE-2017-3462, CVE-2017-3463, CVE-2017-3464, CVE-2017-3600, CVE-2017-3302, CVE-2017-3305, CVE-2017-3450, CVE-2017-3599, CVE-2017-3452, CVE-2017-3331, CVE-2017-3454, CVE-2017-3455, CVE-2017-3457, CVE-2017-3458, CVE-2017-3459, CVE-2017-3460, CVE-2017-3465, CVE-2017-3467, CVE-2017-3468

  MySQL CPU July 2017: CVE-2017-3646, CVE-2017-3732, CVE-2017-3635, CVE-2017-3641, CVE-2017-3648, CVE-2017-3651, CVE-2017-3652, CVE-2017-3653, CVE-2017-3636, CVE-2017-3633, CVE-2017-3634, CVE-2017-3647, CVE-2017-3649, CVE-2017-3529, CVE-2017-3637, CVE-2017-3638, CVE-2017-3639, CVE-2017-3640, CVE-2017-3642, CVE-2017-3643, CVE-2017-3644, CVE-2017-3645, CVE-2017-3650
- The browser tab now shows the Dell EMC icon. (29654)
- The User interface can now support setting separated time zones for data formatting for each user. (hd-37435)
- There is now a Common Setup Task that checks whether the user's browser has a PDF reader, which is necessary for reading reports. (29327)
- The file selection and upload widget no longer requires Flash. The widget now uses HTML5. (30547)
- The sort priority of columns within reports is now more consistent among the columns with default sort priority. It sorts the leftmost column first and then the sort priority moves left to right. (30632)
- The Network Status field can no longer be manually edited for any device. (hd-37530)
- You can now override the maximum rows that can be queried in a portlet. (hd-37437)
- You can now multi-select configurations within the Configuration Files portlet and export the selection. The selected files are add to a zip file that can then be downloaded. (hd-31998)
- The Groups portlet can now auto-populate the resource manager as a context broadcaster. (hd-37438)
- The "Firmware Image" Common Setup Task was renamed to "Upload Firmware Image." (30560)
- The growl messages displayed in the upper right corner for a few seconds are now saved to the My Alerts list for viewing later. (30620)
- The "OS Image" label was replaced "Firmware Image" in the Quick Navigation portlet. (29891)
- The "Backup Config" option was replaced with "Managed Resource Configuration Backup" from the Quick Navigation portlet. (29890)

- The Getting Started and Common Setup Task portlets were updated to reflect a Requirement Tag. (30559)

  These tags include Optional, Recommended, and Required. Tool tips describe each tag.
- Device discovery can now read a file containing a list of IP addresses, IP ranges, and/or subnets. (hd-37442)
- When the Resource Manager and Connected Devices portlets are on the same page, you can configure the Connected Devices portlet to get its context from the Resource Manager portlet. This means a row selected on the Resource Manger dynamically drives and populates elated content in Connected Devices. (29885)
- Access to the Domain Access Control menu Item for Managed Resources, Ports, and Interfaces is now managed by the Domain Assignment Write permission. Those upgrading from before OMNM 6.5 SP1 will need to grant the Domain Assignment permission to appropriate roles to re-enable access to Domain Access Control. (29935)
- Blank page is opened when Right Click on discovered device and select New from HOME page. (30839)
- Right Click on Discovered Device does not pop up all contents/options it has. (29961)
- Plugin Blocked even through flash enabled on Browser (30842)
- The following new permissions are added: Update Traffic Configuration, Show Traffic Configuration and Domain Assignment permission.

  If you upgrade your installation and new permissions are available, edit the Administrator Role, and notice an enabled Add button indicates new permissions are available. By default, upgrades turn off any new permissions, so if you want them enabled, particularly for Administrators, click Add and enable them for the Roles for which you want them enabled. (30428)

Resolved Defects and Known Issues

- OMNM **does not** currently support deployment of Cisco Nexus devices. (30812)
- S4112T model fails deployment when using telnet. (30793)

  Workaround: Use SSHv2 to deploy S4112T model.
- When deploying to a stacked N-Series, the device reports the following:

  `Stack port errors detected on the following interfaces″`

  This message causes the OMNM deploy process to state that the deploy failed. (30279)

  Workaround: Check the firmware version on the device to see if the upgrade succeeded.
- Due to OS10 firmware issues with the S4148T model, OMNM discovers only 4 ethernet ports. As a result, sflow and performance data collection does not work properly in OMNM. (30735)
- Discovery profiles that were created in OMNM 6.2.x are missing “Enable SNMP Traps”, “Opt-In to Dell EMC SupportAssist”, “Call Dell EMC server to retrieve

device warranty information", and "Refresh Hierarchical View Membership" actions. (30385)

Workaround: Create a new discovery profile or edit existing profiles and add above listed missing actions.

- In rare cases that the application server may fail to start up after a fresh installation. The software will attempt start the application server up to three times. If this issue is encountered on a fresh installation with a unexpired license, allow 30 minutes to elapse and then reboot the server or VM to resolve the start up issue. (30363)
- On rare occasions, the application server fails to initialize due to one or more DEPOLOYMENTS IN ERROR. (29964)

  Workaround: Restart both the application server and the Web server.
- When uploading a license file, the related view may not update, which prevents you from completing the upload. (30749)

  Workaround: Click on another tab within the view and then return to the tab containing the Choose File/Select License button. This updates the view and allows you to continue.

- EOL report generates the following error when executed: (30742)

  `java.lang.IndexOutOfBoundsException: Index: 5, Size: 4`

  Workaround: The steps you take depend on whether you removed the EOL Report Template Before an Upgrade or After an Upgrade.

  Before an Upgrade

  1. Delete EOL report template from Report Template portlet.
  2. Delete all EOL reports from Reports portlet.
     a. Maximize the Reports portlet.
     b. Select the EOL report.
     c. Expand “EOL Report All Devices” in the reference tree.
     d. Expand “EOL Report Template.”
     e. Expand “Report Group.”
     f. Right-click on a report and then select Delete.

  After an Upgrade

  If you upgraded OMNM and did not delete the EOL report template with associated reports before upgrade, follow these steps:

  1. Delete all EOL reports from the Reports portlet.
     a. Maximize the Reports portlet.
     b. Select the EOL report.
     c. Expand “EOL Report All Devices” in the reference tree.
     d. Expand “EOL Report Template.”
     e. Expand “Report Group.”
     f. Right-click on a report and then select Delete.
  2. Edit the EOL report template to include the System Object Id.
     a. Right-click on the EOL Report Template, and then select Edit.
     b. Select the Source tab.
     c. Move System Object Id from the Available Column to the Selected Column.
     d. Click Save.
  3. Run the report again.

New Features/Devices Supported in 6.5

- Driver support added for Dell EMC Networking models N11XX, N2128PX, N3132PX. (28613)
- Added 6.4 firmware support for Dell Networking N1xxx, N2xxx, N3xxx, N4xxx models. (30171)
- Driver support added for Cisco 2960X-24TS-L. (32118)
- Dell EMC Networking PCT and FTOS drivers support PVID. (29211)
- Driver support added for HP J9470A, J9471A, J9477A, J9623A, J9624A, J9625A, J9626A, J9627A, J9727A, J9729A, J9772A, J9773A, J9774A, J9775A, J9776A, J9778A, J9781A, J9782A. (29374)
- Many reported installation issues have been resolved including:
  - Compatibility mode is no longer required for Win2012/win2016
  - No pre-requisite linux libraries
  - NO UAC requirement
  - Locked file issues have been resolved
  - Detects invalid install dir and provides resolution
  - Improved silent install for Linux and Windows
  - OS Permission issues when installing on to other or non C drives was resolved. (28748)
- The installation was simplified with a new Express installer option. The user simply selects the number of devices to manage and the OMNM installer auto sizes the environment. This eliminates additional installation prompts.
- The installation was improved to include:
  - Automatic check for conflicting MySQL service and abort if found.
  - Automatic modification for the required firewall ports for both Linux and Windows
  - Disk space required is auto- checked
  - New server status console shows status of the Application, Web, and DB servers
- OMNM now checks for third party “MySQL” service during fresh install or upgrade. If the MySQL service is already running, OMNM stops the service and OMNM creates/starts its own MySQL service. (28817)
- The installer is now a single self extracting executable file for either linux or windows. There is no longer a zip file to extract.
- UPGRADE - The following notice was added to the installation when upgrading from 6.2.x to 6.5

  The upgrade procedure you are about to execute changes and migrates data from the previous version of OpenManage Network Manager.

  WARNING: This migration could take from 20 minutes up to several hours to complete, and is based upon the size of your database.

  If necessary, you may click Cancel now to safely abort the installation and re-execute the installation/upgrade at a later time.

  If you choose to continue with the upgrade, DO NOT Abort the database configuration process or there is risk of db corruption.

- Context portlets - This feature is used throughout OMNM and is now user customize-able. Some portlet can broadcast the row selected and some portlet can listen to the broadcast and update accordingly. This can be seen on the resources page between the Resource Manager and the Port or Interface portlet. The Port or Interface portlet only populates if a row on the Resource manager is selected. Click the wrench icon on a portlet to see the broadcasting or listening state.
- Java- less Direct access Terminal. Browser configuration is problematic for java apps. In 6.5 there is a new Implementation that does not require java. The prior Terminal called Java is still available. The new terminal window is a pop up and any number of independent terminal session can be up at the same time.
- A new post discovery Action was added to the default discovery profiles. This action automatically attempts configure the discovered device to enable snmp v2 traps as well as set OMNM as the trap host. This is supported for limited devices which includes: Dell FTOS, Dell DNOS, Dell W-Series/Aruba Controller, Dell W-Series/Aruba IAP, Cisco IOS, Cisco XR, Junos, Edge Core and Ruckus devices. (29404)
- GUI changes - The GUI was modified to the new Dell EMC logo and color along with a change to a horizontal menu. The menu items and portlet in each have been modified. Some naming was modified.
  - Visualizer is now topology
  - Containers is now Hierarchical
  - File Management is now Configuration Management
  - Proscan is now Compliance
  - Event Processing Rules are now referred to as Automation and Event Processing Rules
- GUI Improvement - Adjustable Column widths and re-ordering of columns are now supported within portlets. Click the wrench icon and go to Columns tab to modify.
- Ease of use - A new on-boarding portlet was added to the home page called “Getting Started.” This portlet is intended to get users up running quickly by walking through the typical on-boarding tasks.
- SupportAssist - Direct communication with Dell EMC support for FTOS AND PCT (DNOS) devices that provides automated, proactive, and predictive technology to reduce troubleshooting steps and speed-up resolution time. When activated, OMNM applies configuration to target device(s) to start sending information to Dell.
- TFA configuration of a device was simplified in OMNM So you don't need to manually log into a device to configure it for TFA. You can auto configure flows at the top and port or interface level Supported Drivers: Force10 (excluding the MIOA devices), PowerConnect, Juniper, Cisco. (30023)
- All summary portlets now allows multiselection. (29056)

- In OMNM 6.5 license registration was enhanced to support two license registration actions. If you intend to extend an existing license, choose Extend License Expiration. This results in the new license being activated when the existing license expires. Otherwise if you want to increase the number of resources that you can have under management, choose Increase License Count. This results in the new license being activated immediately. As a result the count from the existing license is combined with the new license to increase the number of resources that you can have under management. (28904)
- License expiration behavior was improved to eliminated the need for a command line installation when the license has already expired. You can now use the GUI interface to install the license (Settings > Application Configuration Settings portlet > License Management) (28905)
- Automatically set community string for new devices so they can be discovered. For environments/devices where snmp is not configured, OMNM automatically sets an SNMP v2 community on the target devices so they can be discovered in OMNM (limited driver support).
- A Post discovery action in discovery profiles can auto configure devices to send traps to OMNM. Supported drivers, Force10, PowerConnect, Juniper, Cisco, Aruba.
- Database free space low Event - Database Capacity EPR was added to trigger a critical alarm notification when the Oracle or MySQL DB has capacity <=25%.
- Integration - OMMN 6.5 now supports a rich set of REST APIs for integration.
- Actions - A new action type called “Restful Web service” was added. Users can write a custom JSON script to interact with any device or system that supports REST.
- TFA - Similar to Resource Manager, right click from Topology brings up traffic flow for a specific device.
- New Virtualization - To allow the users of OMNM to provide comparable support for virtual network components as OMNM has traditionally provided for physical network devices the OMNM 6.5 release contains new support for managing Openstack virtualizaiton. 11 new portlet under Add-Applications-> Virtualization Management.
- The Virtual Appliance was improved to automatically configure the OMNM file server. When the virtual appliance setup menu option is executed to configure the VM with its new IP address, the new file sever is also created in the OMNM db. After bringing up OMNM for the first time, you will see two file server entries. One is for a TFP/TFP server and the other is for an SCP server.
- In OMNM 6.5 to aid navigation, Additional Filters have been added to Reports, Report Templates, Action and Compliance summary portlets. To select a filter click the wrench icon to create a new Filter or set a new default filter for the portlet. These filters are also available in filer option of the expanded portlet (+ sign upper right portlet) (28994)
- In OMNM 6.5 the default Job Viewer settings were changed to include the option 'Show Informational Messages by Default'. Job Viewer options can be re-configured within the Control Panel under Redcell > Application Settings > User Interface tab. (29520)

- A new Scheduled Maintenance (Next 30 Days), Historical Maintenance Log, & All Future and Historical Maintenance Logs reports and Maintenance Logs Template have been pre-seeded. These reports capture maintenance log entries that have been entered on a managed devices. The maintenance log information can be also seen in detail page of a managed devices under maintenance info tab. (28811)
- Event Processing Rule (EPR) types have been re-categorized. The prior category “Pre-Processing” was split into three new categories “Protocol Translation”, “Stream Based Correlation” and “Event Definition Override”. Each EPR type that was previously within the “Pre-Processing” category was assigned to one of these three new categories on the basis of the when these rules come into play within the event life cycle. The prior category “Post-Processing” was renamed “Automation”. (28493)
- Variable Binding Definitions can now be viewed and edited through a new portlet, which was added to the “Definitions and Rules” page. (28493)
- The Event Definition edit screen was enhanced to allow users to configure service propagation, entity lookup type, mining of variable bindings, and automated parent/child correlation for root-cause analysis. These features could previously only be configured through XML and required the server to be restarted to take effect, but these features are all now fully configurable through the GUI. (28493)
- Automation Event Processing Rules can now have explicit member entities, which is a convenient way of configuring the EPR to only be triggered by events that are associated with these member entities. Explicit membership also allows for the default filter criteria and/or action parameters to be overridden by parameters that are associated with the explicit members. (28493)
- The general discovery profile options were modified to include the “Attempt to enable SNMP” option and “Equipment Type” list for SNMP device configuration. (28812, 29809)
- Syslog escalation was enhanced to allow for alarm suppression and also for the severity of the resulting event to be determined by the severity from the original syslog message. (26090)
- Any event can now be forwarded to a northbound interface as a syslog message or as an HTTP REST call. Northbound forwarding of SNMP traps is still supported so now users can choose from any of these three message types when creating an Event Processing Rule to forward events northbound. (27926)
- Traffic Flow Application names can now be edited. This is useful if custom L7 applications are used. In prior versions, only the L4 protocol name and port number should show for custom application names, but these can now be edited through the GUI. (28596)
- In the expanded traffic flow portlet, in the table of aggregate values that appears below the line graph, the values now have a higher degree of precision. In previous versions, these values were rounded to the nearest whole number, but now the values can include fractions of up to two decimal places. (27506)

- More configuration options have been added to the expanded Traffic Flow portlet. Users can now choose whether or not to use cache tables for queries and also whether to put a limit on how many conversational flows per minute should be processed. Both of these options give more flexibility in dealing with high-volume scenarios. These options were available in previous versions, but activating them required users to edit text files and restart the server. They are now fully configurable through the GUI. (27323)
- The portlet settings button, which shows a wrench icon and through which users can edit the settings for portlets, are now only accessible for users who have the "Change Portlet Settings" permission. On upgrade, no users will have this permission. This is by design, because the intent is for the system administrator to consider which users (more specifically, which user roles) should be able to change portlet settings and which users should not have access to this feature. (3463)
- OMNM can now display information gathered by OpenManage Essentials (OME). If you are already using OME to manage computer systems such as servers, etc. then it is possible to configure OMNM to synchronize with OME so that all of your data is available through OMNM. (28617)
- OME integration includes the option to poll for alerts from OME, which then appears as events and/or alarms in OMNM, but not all attributes of the alerts in OME will translate to attributes in OMNM. For instance, if an OME alert was acknowledged then this would not cause the equivalent OMNM alarm to also be automatically acknowledged. (29208)
- You can configure OMNM to synchronize with the warranty information in the Dell EMC database for each Dell EMC device that is under management. (28909)
- If it happens that there is a communication failure between the system and an external server or remote service, it now creates an alarm that records what failed and what operations were impacted by the failure. This includes attempts to communicate with an external file server, email server, HTTP proxy server, or a remote website. (29488)
- New Device Support
  - Alcatel – See Supported Alcatel Equipment on page 46
  - Aerohive - See Supported Aerohive Equipment on page 46
  - Edge Core - See Supported Edge Core Devices on page 61
  - EMC Unisphere - See Supported EMC Unisphere Devices on page 61
  - Ruckus - See Supported Ruckus Devices on page 64

Resolved Defects and Known Issues

- When upgrading to OMNM 6.5 the default trial package automatically installs the trial license increasing the allowable managed device count by 25. This additional 25 are free to use but will expire 30 days from installation returning the device count back the original subscription device count. A notification banner shows that 25 will be expiring in X days. (29012)
- Initial discovery of Cisco XR devices could fail while configuring the SNMP trap settings on the device. This could be because the application couldn't login to the devices as the number of cli sessions to the device was maxed out. If this happens, the snmp trap setting can be done by running the snmp task from the actions portlet against the xr device. (29389)

- Safari blocks any and all keyboard input for FlashPlayer applications. As a work around, use Chrome. (29120)
- OMNM requires Flash player to be installed and enabled in order for all features to work, including license importing, uploading of files, and topology views. You will need to configure your browser to always activate Flash. For Chrome, go to Settings > Advanced > Privacy and security > Content settings > Flash > Ask first > turning off. For Firefox, it should display an option in the upper left that asks if you want to enable Flash always or just this once. Select always enable. (29413)
- Uploading files into OMNM, such as XML and MIB files, is a two-step process. Starting from the file upload popup dialog, the first step is to select a file from the local file system and the second is to push the button to upload the file. There is a known issue where sometimes after selecting a file, the upload button is still disabled. This issue is caused by a bug within the Flash plugin. If this does happen then you will need to select the file again and then the upload button should be enabled and you can complete the upload process by clicking this button. (29413)
- Do no use IE on Windows 2016 server because it does not support flash. (29829)
- When upgrading to OMNM 6.5 the default schedule item for processing Change Determination is replaced. As a result the scheduled execution time and enabled state may need to be reconfigured to retain the previous behavior. (29620)
- When configuring ports and interfaces of Juniper devices that utilize jflow version 9, the current assumption is that the target ports either already have an inet address configured or is assigned an inet address by dhcp. (30132)
- End user receives a `Cannot find CLI Authentication` message during the SNMP trap configuration. This message is inaccurate, it should read “SNMPv3 is not supported for trap configuration.” (29990)
- Executing remove configuration against a Juniper device with only one flow-server will result in an error being thrown due to the inline-jflow configuration requiring at least one flow-server. Removing the last flow-server will require the user to either directly access the device for manual configuration or to create an Action that executes the required commands to remove both the flow-server and the inline-jflow. (30111)
- Configuring the Flow-samplers for Cisco IOS Devices can be done using the following Actions: Cisco Device Configure Flow-Sampler and Cisco Device Remove Flow-Sampler for device level configuration, Cisco Port Configure Flow-Sampler and Cisco Port Remove Flow-Sampler for port level configuration. (30185)
- Fans and power supply are now being discovered for Dell EMC Networking devices and Dell EMC Networking FTOS devices. (36464)
- For OMNM 6.5 linux installation, internet access is required to do an upgrade to 6.5. A yum command (yum -y install libaio) is required during the install process. If internet access is not available for the OMNM server, the libaio package needs to be manually installed prior to installation. (28065)

- If you have created custom Action scripts using perl you may encounter execution or compilation errors similar to the ones show here. Note that Pre-seeded perl action scripts in OMNM still runs as expected without this issue.

  Cannot load '`/usr/lib/perl5/5.22/i686-cygwin-threads-64int`...'

  or Compilation failed in require at `/usr/lib/perl5/5.22/i686-cygwin-threads-64int`...

  These are due to issues with the embedded perl version 5.22 where numerous libraries have been omitted. The work around is to revert to Perl version v5.14

  Workaround on Windows - Use Prior Perl Version 5.14

  Set Perl to use version 5.14 by executing the following commands from an Oware prompt:

  ```
  mv -n ~/oware3rd/cygwin/bin/perl.exe ~/oware3rd/cygwin/bin/perl.exe.ORIGINAL
  cp ~/oware3rd/cygwin/bin/perl5.14.2.exe ~/oware3rd/cygwin/bin/perl.exe
  perl --version # Confirm that version output contains: v5.14.2
  ```

  Confirm that following script runs OK (or use your script)

  ```
  perl ~/owareapps/performance/scripts/http_test.pl
  ```

  To set Perl back to version 5.22 execute the following commands from an Oware prompt:

  ```
  cp -f ~/oware3rd/cygwin/bin/perl.exe.ORIGINAL ~/oware3rd/cygwin/bin/perl.exe
  perl --version # Confirm that version output contains: v5.22.1
  ```

  Confirm that following script FAILS with 'Compilation failed'

  ```
  perl ~/owareapps/performance/scripts/http_test.pl
  ```

  This issue will be resolved in OMNM 6.5 SP1 by moving to a newer perl version. (30032)

New Features/Devices Supported in 6.2 Service Pack 3

- Added 9.11 firmware support for Dell Networking FTOS models: S6100, S6010, S4048T-ON, S3100, S3148, S3124, S3124F, S3124P, S3148P, IOA/MXL, FX2 IOA, S4810, S4820T, S5000, S6000, Z9500. (28755)
- Driver support added for Dell Networking N3132PX model running 6.3.5.x firmware. (28768)
- Driver support added for netgear. Supported models include FS726T, FS726TP, FS728TP, FS728TPv2, FS752TP, FSM7226RS, FSM7250RS. (28699)
- A Logs tab is now exposed when navigating to the equipment details panel > (example Resource manager > details or topology > detail). The logs tab allows you to enter free form maintenance log information that can be reported on. (28777)

Resolved Defects and Known Issues

- The backup-config file must be created first for backup to backup-config to work properly for N3132PX model. To do this, end user must either create this (backup-config) file directly on the device or execute copy running-config to backup-config or startup-config to backup-config ACLI. (28784)
- Permission issues caused by license - You receive the `You do not have a permission to view this application` message, it most likely means that you have an expired feature license.

  Solution:

  For Virtual Appliance:

  1. Re-apply vmlicense.xml located in the /home/synergy directory
  2. Apply the Dell generated SKU license if you received one.

  For Non Virtual Appliance:

  1. Re-apply the license.xml file located in the ..\OpenManage\Network Manager directory
  2. Apply the Dell generated SKU license if you received one.
- In some cases on Windows OS, if you try to install on a mapped local drive the install will fail because of insufficient write privileges. This can occur even when the user is a member of the administrator group. You can recover your installation with the following steps. It is best to verify that these privileges exist before starting the install. (20321)
  1. CHANGE: file permissions to “Include inheritable permissions” on directory: *...\oware3rd\mysql\data\mysql*
  2. STOP: Web Server via GUI.
  3. STOP: App Server via Windows Task Manager -> End Java Process.
  4. RUN: following commands from oware prompt:

     ```
     net stop mysql && net start mysql
     mysqladmin.exe -u root password dorado
     loaddb -d -m -q
     loaddb -s
     ocpinstall -s -d
     ```
  5. START: Web and Application Servers from GUI.
- When restore running config with no reboot is selected against N-Series while using SCP file server, OMNM will timeout, but the restore will be executed on the device. (32017)
- The MySQL default listener port (3306) **is not** being restricted to only local traffic leaving the OVA users exposed. (30777)

  Workaround: Block external access to MySQL for the OMNM Virtual Appliance by issuing the following Linux shell commands to prevent remote access to MySQL by blocking port 3306.

```
sudo iptables -D INPUT 7-p tcp --dport 3306 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 3306 -s localhost -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 3306 -s synergy.domain.int -j
  ACCEPT
sudo iptables -A INPUT -p tcp --dport 3306 -j DROP
sudo service iptables save
```

- MySQL passwords are not secure. (30777)

  Workaround: Secure MySQL passwords for all OMNM versions using the following steps to change the MySQL root and application passwords. These procedures also prevent the MySQL root password from being stored in configuration files and obviates MySQL root access by the application.

  1. Stop web and application servers.
  2. Change the MySQL root password.

     This password is **not** stored in any application configuration files.

     Example MySQL commands:

     ```
     SET PASSWORD FOR 'root'@'%' = PASSWORD('SecretRootPassword');
     SET PASSWORD FOR 'root'@'localhost' = PASSWORD('SecretRootPassword');
     ```
  3. Create a MySQL user “synergy” with access to “synergy” and “lportal” databases.

     Example MySQL commands:

     ```
     CREATE USER 'synergy'@'%' IDENTIFIED BY 'SecretAppPassword';
     GRANT ALL ON synergy.* TO 'synergy'@'%';
     GRANT ALL ON lportal.* TO 'synergy'@'%';
     ```
  4. Change the MySQL password used for application access by “oware” and “owmeta” users.

     Example MySQL commands:

     ```
     SET PASSWORD FOR 'oware'@'%'  = PASSWORD('SecretAppPassword');
     SET PASSWORD FOR 'owmeta'@'%' = PASSWORD('SecretAppPassword');
     ```
  5. Store the MySQL application credentials in the portal-ext.properties configuration file.

     a. Open the following file:

     ```
     .../oware/synergy/tomcat-7.0.40/webapps/ROOT/WEB-INF/classes/
       portal-ext.properties
     ```

     b. Update the following properties:

     ```
     jdbc.default.username=synergy
     jdbc.default.password=SecretAppPassword
     ```
  6. Store MySQL application credentials in installed.properties configuration file.

     a. Open the following file:

     ```
     .../owareapps/installprops/lib/installed.properties
     ```

     b. Add/update the following property:

     ```
     com.dorado.jdbc.password=SecretAppPassword
     ```
  7. Start web and application servers

New Features/Devices Supported in 6.2 Service Pack 2

- Driver support added for Cisco LSSB SF 200-xx, SF 300-xx, SF 302-xx, SF 500-xx, SG 500-xx; SG 500X-xx models. (28388)
- Added 6.3.0.19 firmware support for Dell Networking N1xxx, N2xxx, N3xxx, N4xxx models. (28389)
- Web links were added for end users to download FTOS and DNOS firmware:

  To execute FTOS firmware download feature, go to Image Repository and right click within a table and select Download Firmware for/Dell FTOS. Log into a website and proceed to location of desired FTOS series to download the firmware.

  To execute DNOS firmware download feature go to Image Repository and right click within a table and select Download Firmware for/Dell DNOS. Click on “Choose from all products.” link and select desired switch. (28391)
- The following monitors were added: Cisco Ethernet SLA, Cisco IP SLA, Cisco QOS, Juniper COS, Juniper RPM. (28136)
- IPSLA monitor now supports class of service TOS threshold alarms. (3746)
- Polling data from IP SLA monitors can now be filtered by SLA key and/or TOS. (20304)
- Traffic Flow Analyzer now supports IPFIX. (27240)
- Traffic Flow Analyzer was enhanced to allow for grouping and querying for exporters by equipment manager and by subcomponent (port or interface). The Traffic Flow Exporters summary portlet now shows the exporters by equipment manager only. From the Managed Equipment portlet, selecting the “Show Traffic as Exporter” menu item will navigate to the maximized Traffic Flow portlet and the context will be set to show the traffic flow data for the selected equipment manager. A new “Traffic Flow Analyzer” menu group was added to both the Ports and Interfaces portlet, which expands to show the menu item “Show Traffic” which when clicked will navigate to the expanded Traffic Flow portlet and the context will be set to show the traffic flow data for the selected subcomponent. (27394)
- Reports for Traffic Flow Analyzer data can now be filtered by exporter. Each TFA entity type now has two new filter attributes: Exporter Equipment Manager and Exporter Subcomponent (28054)
- Traffic Flow Analyzer was enhanced to allow for querying by flow direction. This information is read from the flow packet (sFlow, Netflow, or IPFIX) and saved to the database. The available options are Ingress, Egress, and Both Ingress and Egress, the latter of which is the default setting. (24935)
- Trend reports can now be generated for Traffic Flow Analyzer data. (28055)
- A new column named 'Deployable' is now added to Monitor status summary panel that says why the target is deployed or not deployed. (28070)
- Network Topology was enhanced to preserve link coordinates in saved topology views. (3340)
- The field 'Maximum Entities Per Graph' was added to Trend Report Template editor allowing user to set the maximum member of entities shown per graph within trend report. See Report Template Editors in User Guide for more details. (20237)

Resolved Defects and Known Issues

- Security vulnerability: Linux Kernel Privilege escalation vulnerability - CVE-2016-519

  aka Dirty Cow a Linux OS vulnerability. The vulnerability Impacts Redhat and Centos Operating systems where OMNM is installed.

  For resolution on Redhat refer to: https://access.redhat.com/security/vulnerabilities/2706661

  For Centos 6/7 run `"sudo yum update kernel"`

  The OMNM Virtual Appliance with OMNM 6.2 SP2 on Centos 6.5 was updated and verified as resolving the vulnerability. (20674)
- Google Maps were not loaded properly. Refer to Using Google Maps section in User Guide for more details. (20461)
- The internal file server is locking the password for minutes at a time, so as a result, the deployment will fail for some of the devices. That is why we state in documentation to use internal file server for lab/test purposes and external file server for live network purposes. (11591)

New Features/Devices Supported in 6.2 Service Pack 1

- Driver support added for Dell Networking FTOS models: S6010, S4048T-ON. (27836) (27838)
- Driver support added for Brocade 6510. (11740)
- Added 9.10 firmware support for Dell Networking FTOS models: S6100, S6010, S4048T-ON, S3100, S3148, S3124, S3124F, S3124P, S3148P, IOA/MXL, FX2 IOA, S4810, S4820T, S5000, S6000, Z9500. (27757) (28042) (27909)
- Added firmware 3.0.0.70 support for Dell Networking X-1000 Series switches. (28043)
- Devices running 9.10 firmware version or newer are collecting KPI information using SNMP protocol. Since older firmware doesn't support KPI information using SNMP protocol, OMNM still needs to use CLI to retrieve information from the devices. (27757)
- The EOL Report ALL Devices report was pre-seeded with Force10 end of life(EOL) and end of service(EOS) dates. In event of upgrade, these dates will override the pre registered EOL/EOS dates of Force10 models. See Network Assessor Reports section in the User Guide to update your EOL/EOS dates. (27759)
- Zero-touch provisioning is a process through which devices can be automatically configured and provisioned. Auto-discovery is a related process through which Dell OpenManage Network Manager automatically discovers unmanaged devices that have been configured to send traps.

  To enable zero-touch provisioning within your network, you will need an external DHCP server. This server needs to be configured to automatically provision new devices with a basic configuration file. You can include any basic configuration settings you want within this file. See the Zero-Touch Provisioning and Auto-Discovery section of the User Guide for information on how to activate auto-discovery of network devices within OMNM. (28022)

- You now have the ability to add a language portlet to any page. This portlet allows you to change the language that OMNM displays.

  The home page now shows a language portlet that allows you to change the language that OMNM displays. This allows any user to select their preferred language by clicking one of the buttons and this will take effect right away and it does not affect any other users. By default, there are buttons shown for English, Spanish, and French. This portlet can be configured to show different language buttons by clicking on the wrench icon in the upper right and then selecting Configuration. From the popup window, you can change the language options that are shown within the portlet. Note that even when you change the language, some content will remain in English. For Spanish and French, most of the content was translated and for other languages such as Chinese, Finnish, Portuguese, etc, only a small portion of the content was translated, but it is possible to configure OMNM to show all content in one of these languages. See the Localization chapter of the User Guide for information on how to do this configuration. (27818)

  In addition to the Language portlet the following portlets are available to be added to a page:

  - Dictionary (helps you look up words and uses Dictionary.com)
  - Network utilities (simple DNS lookup and whois, which is to lookup autonomous system names and numbers)
  - Password generator (creates a password string that you can choose to use if you want, but this portlet has no effect on authentication by itself)
  - Quick Note (lets you enter notes)
  - Search (searches the media postings within OMNM)
  - Sign In (displays the name of the user who is currently signed in)
  - Unit converter (calculates unit conversion)
  - iframe (makes it possible to embed another HTML page inside the current page)
  - web proxy (allows showing any website or any content accessible using HTTP as if it was a portlet)
- Added ability to export performance graph to CSV. There is an export button to each chart in the launched dashboard, when the button is clicked a job is created and a message is created in the My Alerts when the csv file is ready. Clicking on the magnifying glass next to the “Performance CSV report is now ready for viewing” message causes the file to be downloaded. (28014)
- You can now copy a report templates. (27802)
- The Canvas Line Charts option controls the type of line charts that are used. Earlier versions of Dell OpenManage Network Manager used a Scalable Vector Graphics type line chart. Now it supports a Canvas based line chart which can display many more points. If you prefer to use the old style SVG line charts you can uncheck this box. Please note that in the expanded traffic analyzer portlet the Export to PDF option is not available for canvas based line charts. If you need to use this feature you should uncheck the box. (27920) (28057)
- The ability to exclude a specific IP address on discovery profiles is limited to IPv4 only. IPv6 discovery at this time does not support ranges or subnets so exclusion is not necessary. (27765)

- Resource Monitors of the type SNMP Interfaces now have new filterable attributes, Monitor Target Name and Monitor Target Description. These will automatically be applied to all newly created monitors. For existing monitors, you will need to perform a manual action in order for these new attributes to be applied. Simply go to the Resource Monitors portlet and select each enabled monitor and edit the monitor and re-save it (you don't need to change anything on the edit screen). Do this for each monitor that you wish to have the attributes available. In some cases the list of available attributes for each monitor will be cached on the web server, so even after you perform this action, it might not take effect until the web server is restarted. These new attributes can be used when viewing and filtering monitor data and also when applying a filter to a report that uses monitor data. (2941)
- A new calculation type called Min/Avg/Max was added to the report templates. If you assign this to at least one attribute it will create a report summary at the top of the report. If there is a date attribute in your report columns it will show the date range (start and end times) in the report summary. If you have report groups enabled a group summary will be created for each group. (3736)

Resolved Defects and Known Issues

- Fixed issue where upgrade sometimes revert the user's customizations layout. (27778)
- OMNM 6.2 SP1 - action group doesn't have a help page. (28032)
- The following vulnerabilities have been addressed with an updated SSL component in the product (3898, 11579)

  CVE-2016-0800, DROWN

  CVE-2016-0702, CacheBleed

  CVE-2015-3197. SSLv2 doesn't block disabled ciphers

New Features/Devices Supported in 6.2

- Driver support added for Dell Networking W-series: W-7205, W-7024, W-7240XM, W-IAP277, W-IAP228, W-IAP205H, W-IAP324, W-IAP325, W-AP228, W-AP205, W-AP324, W-AP325, W-AP277. (27756)
- Driver support added for Dell Networking FTOS models: S6100, S3100. (27754) (27755)
- Z9100-ON support for Dell FTOS 9.8. Cumulus linux not supported. (27752)
- Driver support added for Arista. (27771)
- IP v6 is now supported. (27447)
- Oracle 12c R1 (12.1.0.2.0) is now supported. (26356)
- Seeded ACLIs can now be copied. (27924)
- Graphing min/max aggregate values in dashboards is now supported. (6350)
- A new set of pages have been added to provide Quick Network Assessment Views of the network. These pages contain OMNM portlets arranged for a Quick View Assessment. The Parent page, called Network Assessment, is located below the Home page and contains topology view, select Performance Monitor portlets and executive Reports. Network Assessment has Sub menu called Performance Assessment and is also a select set of PM portlets. Network Assessment has Sub

Menu called Traffic Assessment with a select set of Traffic Flow Analyzer portlets. (27261)

- VMWare ESX and KVM Controller Support

  Basic support for management of VMWare ESX and KVM Controller devices was added. The controllers are discovered/managed via WBEM protocol and require WBEM and SSH authentication protocol at discovery time.

  VMs will appear in the controller's reference tree, but can also be discovered standalone.(27782) (27783)

- Localization of decimal point as a comma is now supported because many countries use a comma for the decimal point rather than a dot. For example, a number formatted in the US and most English speaking countries as 459.12 would be 459,12 in countries such as Mexico, Argentina and Morocco. (27813)
- License enabled for all action types include Configure Commands, External Executable, Show Commands, Config File Generation, Perl Script and Script Only Generation. (27796)
- Prior version of OMNM had vendor-specific performance monitors that were seeded by the system during installation. These were named "Default Cisco Monitor" and "Default Juniper Monitor". OMNM 6.2 no longer seeds these monitors during installation, but if these monitors were seeded during the installation of a prior version, they will still function properly. These monitors are no longer seeded because OMNM 6.2 seeds performance monitors that perform the same function and are work for all devices, regardless of vendor (including Cisco, Juniper, Dell, etc.) These vendor-independent monitors are called "Default Temperature Monitor", "Default CPU Monitor", "Default Memory Monitor" and "Default IP Statistics Monitor". All four of these monitors target devices regardless of vendor, so thus the vendor-specific monitors are not necessary. (27912)
- The site management portlet lets you restrict access to configured network domains. Select the configuration icon (the wrench) which opens the Global Site Settings dialog. Here the administrator can add networks that the primary site’s central domain users can login from, or exclusions of things like a proxy server within one of the permitted networks which allows external access to the web server. When attempting to login from an IP address other than those permitted a message appears saying Login is restricted from your current IP [IP Address].

  Notice that you must check Login Restrictions Enabled to begin restricting access. When you check that, global portal users can only log in from defined, permitted networks. You can also elect to Apply Login Restrictions to Portal Admin with that checkbox, too.

  Currently only IPv4 address can be used. If end user wants to exclude all IPv6 addresses, s/he can specify IPv4 range as a permitted network range. If end user doesn't specify any permitted network, then all IPv4 and IPv6 addresses are permitted to see OMNM application.(27948)
- Under OMNM Add -> Applications in the Portal Applications -> Sample section, a new portlet called iFrame is available. You can use the iFrame portlet to link a URL and make it a page within OMNM. (27913)
- Auto Discovery AKA Zero touch provisioning is now supported. This feature allow any device to be auto discovered via DCHP boot or USB boot. refer to the user guide section Auto Discovery via DCHP boot or USB boot for configuration details. (27994)

- Currently, we only obtain service tag information from top (master) device. To report on service tags that belong to stacked (slave) devices, create custom attributes in resource manager to store additional service tags. To accomplish this task, right click on any device and select "Edit Custom Attributes" menu option which opens "Custom Attributes Editor" form. Click on edit button that is associated with "String" Type and fill in appropriate information and click on "Apply" button to save the settings. Repeat the process for multiple sting types. Now, you are ready to create an ACLI that will provide additional service tags of stacked devices upon execution. To accomplish this task, right click on any row in action portlet and select "new/Adaptive CLI" menu option which will bring up "Creating New Adaptive CLI" form. Type in name and click on "Add" button where you select the appropriate vendor. After that click on "Apply" button. In "Scripts" tab click on "Add New Script" button and select "Embeded CLI" menu option. Type in 'show system id' and click on "Apply" and "Save" buttons to save created ACLI. Right click on created ACLI and select "Execute" menu option that allows you to execute created ACLI against stacked devices. Once the ACLI is executed, make a note of the additional service tags that are now ready to be added to the appropriate devices. To accomplish that task, edit appropriate device in resource manager and add noted service tags to the custom fields and save the device. At this stage, you are ready to create a service tag report. In report template manager, right click on any row and select "New/Table Template" menu option. Fill in a name, in "Source" tab select "Inventory Resource/Managed Equipment" and add created custom attributes to selected columns. Add any additional attributes that you want to see on the report and save the template. In report manager, right click on any row and select "New" menu option. Type in a name of the report and save the report. Now you can execute the report to see additional service tags. (11053)

Features/Devices Supported in 6.1 Service Pack 1

- Driver support added for Dell Networking FTOS models: S6000-ON. (27704)
- Driver support added for Dell Networking W-series : W-7205, W-7024, W-7240XM, W-IAP277, W-IAP228, W-IAP205H, W-IAP324, W-IAP325, W-AP228, W-AP205, W-AP324, W-AP325, W-AP277.

Features/Devices Supported in 6.1

- Driver support added for Dell Networking X-series switches: X1008, X1008P, X1018, X1018P, X1026, X1026P, X1052, X1052P, X4012.
- Driver support added for Dell Networking model: PowerEdge VRTX 10Gb.
- Added 6.2.6.x firmware support for all Dell Networking N-Series models. (27236)
- Driver support added for Dell Networking FTOS models: C9010. (27138)
- Driver support added for 3com: 5500 EI Switch Series (JD377A) Router.
- Driver support added for Cisco IOS: 3750_48 and 3850-48P-S Switch.
- Driver support added for Cisco IOS-XR: 12816(XR) and CRS1-Fabric Router.
- Driver support addedfor Cisco MDS: MDS 9509 Fibre Channel Switch.
- Driver support added for Cisco Nexus: 2248G, 3548, 5596T and 7718 Switch.
- Driver support added for Cisco PIX/ASA: Cisco ASA 5585-X SSP-60 and Cisco PIX Firewall 535sy Firewall/VPN Appliance.
- Driver support added for Cisco LSSB: 24-Port 10/100 Managed Switch. (27306)
- Driver support added for Extreme devices. supported model included Alpine 3808, Black Diamond 12804 and Summit 1iSX Switch.
- Driver support added for HP ProCurve: J9623A Switch E2620-24. (27304)
- Added support for Cumulus. The supported version of Cumulus Linux is 2.5. support any model that run Cumulus Linux.
- Added support for SonicWall devices. Supported models include Generic SonicWALL, NSA and TZ series. (23502)
- Added support for Vyatta devices. Firmware supported 1.0.x, 6.6.x & 6.7.x for model Vyatta Firewall 5400.
- High Availability installation, Oracle Database support. Refer to Installation Guide for details.
- Extended Event Definitions, Action Groups, Pre-seeding EOL Report, Export to Visio, Radius support, Find Physical Connection for IP or MAC Addres, Multitenant support. Refer to User Guide for details.
- The License Generator tool was updated to include support for Enabling HA and Oracle.
- A new OMNM Virtual Appliance is available for OMNM 6.1.
- Fiber Channel Port Statistics information can be obtained using the “Dell Networking (FTOS) Show Interfaces” ACLI. Please specify the fiberchannel interface as the interface parameter. (27148)
- Permission Updates - After upgrade to OMNM 6.1, you may see a message in Configuration Files portlet that says you do not have permission to view this application. This updated permission permits no access by default and needs to be reset by user. To see or alter them, any administrator user can look in the Permissions in Control panel.

  Go to > Control Panel > Permission Manager > Edit Administrator role > click Add > select 'Configure Files' from the Select Permission list > Check all the check boxes > click Apply > Click Save

  Finally, you must also log out and log back in for any permission change to take effect. (23888)

- ctrl and shift will allow multi select in resource manager minimized portlets allowing delete of more than 1 device at a time.
- The "Alarms by location" page is a context driven view that depends on the pre-configuration and administration of containers from the container manager in the Admin tab. If there are no container configured the Container tree will be empty and the other context driven portlets will also be empty. Refer to the user manuals or search "Help" for "Container manager" for more information. (25373)
- With this release, traffic flow data is automatically converted to a new format that can be inserted into the DB and queried more efficiently. Our testing showed that the original implementation of IP conversations could be improved. This implementation involved a table that had a row for every unique IP conversation (sender/receiver combination, where IP A sends to IP Z is the same conversation as when B sends to A) where the only purpose of this table was to assign a unique ID to each conversation. At some customer sites where they measured all internet traffic going through their network, this table quickly grew to hundreds of millions of rows, and this was a significant performance drag when it tried to insert new data because it constantly had to query this table to see if the conversation is already on record and so it could get the ID. So we came up with a new approach that simply assigned a unique key to each conversation and stores this in the rollup tables. This key is derived from all essential factors that are relevant to the conversation (IP A and Z, protocol, port) and it converts this into a base 64 string so that it can be readable in string format. After upgrade to this new code, all conversation queries will assume the data is in this new format, but if the user had data before then the new data will be lost unless it is converted. When the server is started the first time after upgrade, there will be a thread running in the background to convert the user's legacy data. After this process is complete, the conversation data should be query-able.
- In earlier versions, there were restrictions for what types of managed equipment could be registered as exporters. This was handled by the system property: ta.exporter.types which was set to:

  Router,Switch/Router,Switch,Converged Ethernet Switch,Firewall

  Now this property has no value and instead we have a new property which disables ta.exporter.types and allows all devices to be registered as exporters, regardless of type: ta.exporter.restrictType

  Which is set to false. It is still possible to override these properties so that these restrictions would be back in place. This can be done by setting ta.exporter.restrictType to true and then to setting ta.exporter.types to a list of equipment types.

- Virtualization enhancements
  - VMware or Hyper VM's with windows or Linux OS can be discovered using standard WMI or WBEM authentication protocols.
  - Linux machine Virtual and Physical now support an SSH management interface.
  - ESXi servers that support WBEM can be discovered with WBEM/HTTPS management interface. The inventory of VM's will be discovered and listed in the ESXi servers, reference tree.
- OMNM was validated to support these latest Browsers versions:
  - Microsoft Internet Explorer v11.0
  - Google Chrome V. 41.0.2272.101
  - Firefox v37.0
  - Safari v8
- New Device Support
  - CiscoLSSB – See Supported Cisco LAN Switches Small Business Equipment on page 49
  - Cumulus – See Supported Cumulus Equipment on page 49
  - SonicWall – See Supported SonicWall Devices on page 64
  - Vyatta – See Supported Vyatta Devices on page 65

Features/Devices Supported in 6.0 Service Pack 3

- Added support for Dell Networking models: N1524, N1524P, N1548, N1548P. (27151)
- Added 9.8 firmware support for Dell Networking FTOS models: IOA/MXL, S4810, S4820, S5000, S6000, Z9500, FN 410S/410T, FN 2210S, S3048 ON, S4048 ON. (27237)

Features/Devices Supported in 6.0 Service Pack 2

- Traffic Flow now displays estimates as well as raw data.

  Refer to Enabling Estimated Flows Based on Sample Flows section in *User Guide* or online help for details.
- Installer now checks partition name for length and special characters.

  Refer to Partition Name Limitations section in User Guide or online help for details
- Added support for Wireless Controllers: W-7005, W-7010, W-7030.
- Added support for Instant Access Points: W-IAP103, W-IAP204, W-IAP205, W-IAP214, W-IAP215, W-IAP224, W-IAP274, W-IAP275.
- Added support for Access Points W-AP103, W-AP103H, WAP204, W-AP205, W-AP214, W-AP215, W-AP224, W-AP225, W-AP274, W-AP275.
- Added 6.3.1.8 firmware support for wireless Instant Access Point devices.
- Added 6.4.2.4 firmware support for wireless controller devices.

- Added support for Dell Networking FTOS models Z9500, FN410S, FN410T, FN2210S.
- Added 9.7 firmware support for the following devices S4810, S4820,S5000, S6000, MXL, IOA, Z9000, Z9500, FN410S, FN410T, FN2210S.
- Added 6.2 firmware support for Dell Networking models: N2024, N2024P, N2048, N2048P, N3024, N3024F, N3024P, N3048, N3048P, N4032, N4032F, N4064, N4064F.

Features/Devices Supported in 6.0 Service Pack 1

- Some Force10 Monitor names change, so if any Event Processing Rules require “Force10” (example: in the varbind of a threshold-crossing notification that triggers the rule), ensure you accommodate that name change for upgrade installations.
- When upgrading from OMNM 5.x to 6.x, to get the correct population of device groups, you must delete the Dell PowerConnect Group before doing the upgrade to OMNM 6.0. (24043)
- You must edit and save the default interface monitor for the `Availability Confidence` attribute to appear after an upgrade. (25593)
- This package includes sample Discovery Profiles and Authentications for Dell, Cisco, Juniper, Windows and Linux devices. Alter these to discover such devices on your network.
- The distribution and licensing has changed in Dell OpenManage Network Manager 6.0. The free 10-device version is no longer available. Support continues for existing users on previous versions. Dell OpenManage Network Manager 6.0 is available in 1,3, and 5 year subscriptions at incremental device counts. All existing users are eligible for a substantial discount for a license equivalent to their legacy one. A paid subscription provides access to support and any upgrades that are made available during the subscription period. Please contact your sales representative for more information.
- License expiration now produces a colored warning in the status bar, an alarm, and lets you order license updates by e-mail from within the license management screen.

  When the `communication to server was refused` message appears in your browser, related to some portlets, it may indicate licensing as the source of the application server not starting.

  The License viewer displays expiration dates for critical components. For example, *Oware* is necessary for application server to run. Components that do not display license expiration dates depend on application server for their licensing. A digital Service Tag referring to your license and level of support also appears in License Viewer. Consult the *User Guide* for details. (25757, 25860, 25981)

- Discovery now automatically updates monitor targets by default. Web Service discovery also does not require a discovery profile exist in OMNM before it can trigger discovery. When none exists, web services create a default profile with the supplied parameters.

  If you have updated your system, you must add the Refresh Monitor Targets action to any existing discovery profiles you have created before this is the default behavior in upgraded discovery profiles. (24151, 24477)

- Device Support
  - Brocade – See Supported Brocade/Brocade RX Equipment on page 47
  - Cisco – See Supported Cisco Equipment on page 47

    This comes with two types of drivers:

    CATOS - supports switches that only support CATOS firmware.

    IOS - supports routers or switches that support IOS firmware. It also provides support for Switches that can run both IOS or CATOS firmware. When viewing the Driver information, model OID support will end in .catos or . ios if the hardware supports both. *Note:* Although both may be supported by the hardware, they may not be both supported by OMNM. (25258)
  - Dell–See Supported Dell Equipment on page 50
  - HP – See Supported HP Procurve Devices on page 62
  - Juniper – See Supported Juniper Devices on page 63

  To see supported device models and OS versions, look in the *Manage* > *Show Versions* menu.

The following outlines various features included in this package:

Adaptive CLIs

Cisco—See Adaptive CLIs on page 31 and Cisco Compliance Actions on page 36 below.

Juniper—See Juniper JUNOS Adaptive CLIs on page 32 below.

HP Procurve—N/A

Brocade—N/A

Proscans

Cisco—See the Cisco Compliance Policies below.

Juniper—See Juniper Compliance Policies below.

HP Procurve—N/A

Brocade—N/A

Monitors

Juniper—RPM

Cisco—IPSLA

Filters/Groups

Cisco—Cisco, All Cisco, excluding XR and PIX, All Cisco excluding PIX, vCisco Devices, Cisco IOS 12.0-12.4, Cisco IOS 12.2(33), Cisco Not IOS 12.2(33)

Groups: Cisco PIX, Cisco Routers, Cisco Switches

Juniper—Juniper VPLS MX-Series, Juniper VPLS, All Juniper Routers

Groups: Juniper JUNOS Driver devices

HP Procurve—N/A

Brocade—N/A

Groups: Brocade Vendor Group

Schedules

N/A

Reports

Cisco—Cisco Card Report

Juniper—BGP Groups, BGP Information, Bootp, Bootp Interfaces, ISIS Information, ISIS Interfaces, LDP Information, LDP Interfaces, MPLS Interfaces, OSPF Areas, OSPF Information, RIP Groups, RSVP Interfaces, SNMP Communities, SNMP Trap Groups, Static Routes

HP Procurve—N/A

Brocade—Fabric Basic Report, Fabric IP Address Report, Port Connection Report, Port Zone Membership Report.

Operating Systems

RedHat/CentOS Support—Version 6.4 of these Linux flavors is now tested and approved for Dell OpenManage Network Manager. (23807)

Adaptive CLIs

The following are pre-seeded Adaptive CLIs for Dell OpenManage Network Manager. Open the Adaptive CLI in the Actions portlet to examine the details of how it works

Cisco Adaptive CLIs

```
Cisco IOS Write Mem
Cisco show run'
Cisco show mpls traffic-eng tunnels'
Cisco show ip interface'
Cisco show inventory'
Cisco show ip protocols'
Cisco show mpls forwarding-table'
Cisco show protocols'
Cisco show ip policy-list'
Cisco show mpls ip binding'
Cisco show configuration'
Cisco show mpls interfaces'
Cisco show ip policy'
Cisco show interfaces'
Cisco show ip route'
```

```
Cisco show ip access-lists'
Cisco show ip traffic'
Cisco show hardware'
Cisco show interfaces rate-limit'
Cisco show interfaces summary'
Cisco show interfaces description'
Cisco IOS Class Map create
Cisco IOS Class Map delete
Cisco IOS Create Ext ACL Entry
Cisco IOS Create PrefixList
Cisco IOS Policy Map create
Cisco IOS Policy Map delete
Cisco IOS Write Mem
Cisco Interface Shutdown
```

See also Cisco Compliance Actions on page 36

Juniper JUNOS Adaptive CLIs

```
Juniper JUNOS 'show protocol' xml
Juniper JUNOS 'show policy-options' xml
Juniper JUNOS 'show policy' xml
Juniper JUNOS 'show mpls path'
Juniper JUNOS 'show mpls lsp up'
Juniper JUNOS 'show mpls lsp statistics'
Juniper JUNOS 'show lsp ingress'
Juniper JUNOS 'show lsp egress'
Juniper JUNOS 'show mpls lsp detail'
Juniper JUNOS 'show mpls lsp descriptions'
Juniper JUNOS 'show mpls lsp brief'
Juniper JUNOS 'show mpls lsp'
Juniper JUNOS 'show mpls interface'
Juniper JUNOS 'show interfaces | routing instances' xml
Juniper JUNOS 'show interfaces routing'
Juniper JUNOS 'show interfaces policers'
Juniper JUNOS 'show interaces filters'
Juniper JUNOS 'show interfaces descriptions'
Juniper JUNOS 'show interfaces brief'
Juniper JUNOS 'show interaces -profiles' xml
Juniper JUNOS 'show interfaces' xml
Juniper JUNOS 'show filewall policer' xml
Juniper JUNOS 'show firewall log'
Juniper JUNOS 'show firewall' xml
Juniper JUNOS 'show cos schedulers' xml
Juniper JUNOS 'show cos scheduler-maps' xml
Juniper JUNOS 'show cos rewrite-rules' xml
Juniper JUNOS 'show cos interfaces' xml
Juniper JUNOS 'show cos forwarding-classes' xml
```

```
Juniper JUNOS 'show cos drop-profiles' xml
Juniper JUNOS 'show cos classifiers' xml
Juniper JUNOS 'show configuration' xml
Juniper JUNOS 'show configuration'
Juniper JUNOS 'show class of service' xml
Juniper JUNOS 'show access' xml
Juniper JUNOS show system rollback ACLI
```

HP Procurve Adaptive CLIs

N/A

Brocade Adaptive CLIs

N/A

Standard Change Management Policies

Change Management comes with several policies and actions by default. These include ProScan policies and policy groups, as well as the corresponding Actions for correcting any violations, and Event Processing Rules that automate remedy actions. The following sections briefly describe these.

- Cisco Compliance Policies
- Cisco Compliance Actions
- Cisco Event Processing Rules

⚠ **CAUTION:**

Seeded Proscan policies are not necessarily correct by default. You must specify device targets at least. Given the variance in responses, particularly for Cisco devices, best practice is to test any such policy before you use it.

Cisco Compliance Policies

The following are Cisco Compliance policies included by default with your Change Management installation. Policies listed here are part of Cisco Proscan Policy Groups scanning for PCI, HIPPA, SOX, NSA, and CISP compliance. These appear at the bottom of this list.

COMPLIANCE Cisco Enable Secret—Use enable secret for enable level access to device; PCI 8.4

COMPLIANCE Cisco Finger Service (12.1+)—Disable Finger service; PCI 2.2.2

COMPLIANCE Cisco HTTP Server—HTTP server should not be running; PCI 2.2.2

COMPLIANCE Cisco Finger Service (11.3-12.0)—Disables finger service; PCI 2.2.2

COMPLIANCE Cisco Identd Service—Disable Identd service globally

COMPLIANCE Cisco Timestamps Logging—Use the timestamps service to show date and time on all log messages; PCI 10.2

COMPLIANCE Cisco Disable MOP—Disable MOP support on all Ethernet and VLAN interfaces; PCI.

COMPLIANCE Cisco NTP Redundant Servers—Ensures that more than one NTP server is defined; PCI 10.4

COMPLIANCE Cisco Disable NTP—Disable NTP if not in use; PCI 2.2

COMPLIANCE Cisco PAD Service—The packet assembler/disassembler (PAD) service supports X.25 links. This service is on by default, but it is only needed for devices using X.25; PCI 2.2.

COMPLIANCE Cisco Service Config—Disable autoloading of configuration files from a server; PCI 2.2.2

COMPLIANCE Cisco Password Encryption—The password-encryption service shows user passwords as encrypted strings within the configuration; PCI 8.4

COMPLIANCE Cisco IP Source Route—Disable handling of source routed packets.

COMPLIANCE Cisco SNMP RW Communities—Do not use SNMP Read-Write strings, and only use Read-Only strings with associated access lists; PCI 2.2.3.

COMPLIANCE Cisco TCP Small-Servers (11.2-)—Disables unneeded TCP services such as echo, discard, chargen, etc; PCI 2.2.2

COMPLIANCE Cisco TCP Small-Servers (11.3+)—Disables unneeded TCP services such as echo, discard, chargen, etc; PCI 2.2.2

COMPLIANCE Cisco UDP Small-Servers (11.2-)—Disables unneeded UDP services such as echo, discard, chargen, etc.; PCI 2.2.2.

COMPLIANCE Cisco UDP Small-Servers (11.3+)—Disables unneeded UDP services such as echo, discard, chargen, etc; PCI 2.2.2

COMPLIANCE Cisco VTY Exec Timeout—Set Exec Timeout on VTY ports; PCI 8.5.15

COMPLIANCE Cisco VTY Access Class Inbound—Set inbound access class on VTY ports; PCI 2.2.3.

COMPLIANCE Cisco VTY Login—Enable Login on VTY ports; PCI 2.2.3

COMPLIANCE Cisco VTY Transport Input Limit—Limit Input Transport on VTY ports; PCI 2.3

COMPLIANCE Cisco Set Login on Console Port—Enable login on console port; PCI 2.2.3

COMPLIANCE Cisco AAA Login—AAA login should be enabled; PCI 8.3

COMPLIANCE Cisco BOOTP Server—The BOOTSP server should be disabled; PCI 2.2.2

COMPLIANCE Cisco CDP Service—Disable CDP (Cisco Discovery Protocol) globally

COMPLIANCE Cisco Console Exec Timeout—Set an exec timeout console port; PCI 8.5.15

Cisco tacacs+ enabled

Cisco monitor logging Enabled

Cisco console logging Enabled

Cisco buffered logging Enabled

Cisco SNMP Community String NOT public

Cisco SNMP Community String NOT private

Cisco RADIUS Enabled

Cisco Interfaces MUST have Description

Cisco Banner Enabled

Cisco ACL RFC 1918 space

Cisco ACL Permit Transit Traffic

Cisco ACL Permit RIP

Cisco ACL Permit OSPF

Cisco ACL Permit IGRP

Cisco ACL Permit EIGRP

Cisco ACL Permit BGP

Cisco ACL Deny access to internal infrastructure

Cisco ACL BGP AS Source

Cisco ACL Anti Spoofing

Cisco ACL - Deny special use address source

Cisco session-timeout' Enabled - ALL LINES

Cisco exec-timeout' enabled ALL LINES

Cisco Proscan Policy Groups

The following combine the ProScan Policies described above into groups to scan for compliance.

PCI Compliance for Cisco—This includes the following COMPLIANCE policies: Cisco VTY Transport Input Limit, Cisco VTY Login, Cisco VTY Exec Timeout, Cisco VTY Access Class Inbound, Cisco SNMP RW Communities, Cisco Password Encryption, Cisco Finger Service (12.1+), Cisco Finger Service (11.3-12.0), Cisco Disable NTP, Cisco Identd Service, Cisco AAA Login, Cisco UDP Small-Servers (11.2-)

HIPPA Compliance for Cisco—A policy group. This includes the following COMPLIANCE policies: Cisco VTY Transport Input Limit, Cisco VTY Login, Cisco SNMP RW Communities, Cisco Set Login on Console Port, Cisco Password Encryption, Cisco PAD Service, Cisco HTTP Server, Cisco Enable Secret, Cisco Timestamps Logging, Cisco NTP Redundant Servers, Cisco Finger Service (11.3-12.0), Cisco Finger Service (12.1+), Cisco BOOTP Server, Cisco CDP Service.

SOX Compliance for Cisco—A policy group. This includes the following COMPLIANCE policies: Cisco VTY Login, Cisco VTY Transport Input Limit, Cisco SNMP RW Communities, Cisco Set Login on Console Port, Cisco Password Encryption, Cisco PAD Service, Cisco Finger Service (11.3-12.0), Cisco Finger Service (12.1+), Cisco HTTP Server, Cisco Identd Service, Cisco UDP Small-Servers (11.3+).

NSA Compliance for Cisco—A policy group. This includes the following COMPLIANCE policies: Cisco VTY Login, Cisco VTY Transport Input Limit, Cisco SNMP RW Communities, Cisco VTY Exec Timeout, Cisco Service Config, Cisco Password Encryption, Cisco PAD Service, Cisco HTTP Server, Cisco Finger Service (12.1+), Cisco Finger Service (11.3-12.0), Cisco Enable Secret, Cisco Disable MOP, Cisco Disable NTP, Cisco NTP Redundant Servers.

CISP Compliance for Cisco—A policy group. This includes the following COMPLIANCE policies: Cisco UDP Small-Servers (11.3+), Cisco VTY Transport Input Limit, Cisco VTY Login, Cisco VTY Exec Timeout, Cisco VTY Access Class Inbound, Cisco Password Encryption, Cisco Finger Service (12.1+), Cisco Finger Service (11.3-12.0), Cisco Enable Secret.

Cisco Compliance Actions

Remedial actions are often part of the process of change management. These may be triggered by the Cisco Event Processing Rules, and are included as part of the

Standard Change Management Policies

Compliance Cisco AAA Login—To avoid being locked out of the router, define username and password on the access server before starting the AAA configuration.

Compliance Cisco Finger Service (11.3-12.0 & 12.1+)—Disables the ip finger service.

Compliance Cisco HTTP Server—Disables http.

Compliance Cisco Identd Service—Disables identd

Compliance Cisco IP Source Route—Disables ip source route

Compliance Cisco UDP Small-Servers (11.2- and 11.3+)—Disables PCI UDP Small-Servers (11.2- and 11.3+).

Compliance Cisco TCP Small-Servers—Displace PCI Cisco TCP Small-Servers.

Compliance Cisco BOOTP Server—Disables PCI Cisco BOOTP Server.

Compliance Cisco PAD Service—Disables the PAD service.

Compliance Cisco Timestamps Logging—Enables PCI Cisco Timestamps Logging.

Compliance Cisco SNMP RW Communities—Removes RW community string with user input.

Compliance Cisco Password Encryption—Enables PCI Cisco Password Encryption.

Compliance Cisco CDP Service—Disables CDP Cisco Discovery Protocol.

COMPLIANCE Cisco VTY Transport Input Limit

COMPLIANCE Cisco VTY Login

COMPLIANCE Cisco VTY Exec Timeout

COMPLIANCE Cisco VTY Access Class Inbound

COMPLIANCE Cisco Set Login on Console Port

COMPLIANCE Cisco Service Config

COMPLIANCE Cisco SNMP RW Communities

COMPLIANCE Cisco Password Encryption

COMPLIANCE Cisco PAD Service

COMPLIANCE Cisco NTP Redundant Servers

COMPLIANCE Cisco Enable Secret

COMPLIANCE Cisco Disable NTP

COMPLIANCE Cisco Disable MOP

COMPLIANCE Cisco Console Exec Timeout

Cisco Event Processing Rules

The event processing rules here typically tie Cisco Compliance Policies with remedial Cisco Compliance Actions.

Compliance Cisco AAA Login Remediation—Triggers a task to configure an AAA login.

Compliance Cisco BOOTP Server—Corrects PCI Cisco BOOTP Server compliance failures.

Compliance Cisco CDP Service—Corrects PCI Cisco CDP Service compliance failures.

Compliance Cisco Finger Service—Corrects PCI Cisco Finger Service compliance failure.

Compliance Cisco HTTP Server—Corrects http server compliance failures.

Compliance Cisco Identd Service—Corrects PCI Cisco Identd Service compliance failures.

Compliance Cisco IP Source Route—Corrects PCI Cisco IP Source Route compliance failures.

Compliance Cisco PAD Service—Corrects PCI Cisco PAD Service compliance failures.

Compliance Cisco TCP Small-Servers—Corrects PCI Cisco TCP Small-Servers compliance failures.

Compliance Cisco Timestamps Logging—Corrects PCI Cisco Timestamps Logging compliance failures.

Compliance Cisco UDP Small-Servers (11.3+)—

Juniper Compliance Policies

Packages that support Juniper devices have the following policies:

Juniper FW Filter Private IP—RFC 1918

Juniper Policer DNS—Protect from source address spoofing

Juniper Policer NTP—Protect from source address spoofing

Juniper Policer RADIUS—Protect from source address spoofing

Juniper Policer SNMP—Protect from source address spoofing

Juniper Policer SSH—Protect from source address spoofing

Juniper Policer Small BW—Protect from source address spoofing

Juniper Policer TCP—Protect from source address spoofing

Juniper Recommended Logging—Confirms recommended logging is on.

Juniper SNMP community NOT public — Checks the SNMP community is not “public” closing a potential security hole.

Juniper SNMP community NOT private — Checks the SNMP community is not “private” closing a potential security hole.

Juniper ALL Services Policy—*Note:* this compliance policy will typically be modified per deployment.

Juniper Recommended SSH—Confirms recommended SSH is on.

Juniper Recommended Syslog—Confirms recommended syslogging is on.

Known Issues

General

- While IPv6 is supported some Filter fields may still not fully support IPv6 data entry. These include: in/not in operands. The "ip address" filter attribute is too short to display a full IPv6 address but filter capability is still supported. (27973)
- There is a known issue in OMNM 6.2 where edits of a save file server will un-check the previously saved TFTP server option.This occurs on every other edit of the file server. The work around is to re-edit and save the file server. Validation of the tftp setting should be confirmed by testing backup with a TFTP only device or through the test function. (28006)
- **Linux HA does not support IPv6 as default -** While IPv6 is supported on Windows HA, Linux HA does not support IPv6 as default. To acquire IPv6 on Linux HA, it's suggested that users must follow these steps enable unicast within the Mediation cluster. Apply the configuration changes to all Mediation servers. Please refer to Chapter Troubleshooting Your Application in User Guide for more details. (27978)
- Installation now requires a minimum of 8G RAM.
- Getting "Bad request Error 400" while clicking on the Google link in the Site page. (27582)
- "no protocol " as error message in os image upload page while providing the input in the Remote (HTTP) URL field. (27511)
- Tool tip states "Null is required", should read "Management State is required" in Management State Settings form. (27476)
- Incorrect popup message appears when trying to save duplicate contact. (27472)
- Incorrect popup message appears when trying to save duplicate location. (27471)
- Pop Up message is not displaying after deletion of any contacts/locations. (27465)
- Incomplete pop up Message for Manage options. (27344)
- TFA - exporters should use device names, not just IP addresses. (27386)
- performance - network dashboard - missing green threshold for percent packet loss %% (27171)

- **Login form missing** workaround: (3526, 3765)
  1. Shut down web server.
  2. In a command shell type the following: `oware`
  3. Type `mysql -u root --password=dorado` This will log you into mysql database
  4. Copy and paste the following into mysql shell and hit enter:

     ```
     update lportal.layout set typeSettings = 'layout-template-
     id=1_column\ncolumn-1=58,\n'
     ```

     where (`groupId=10180`)

     AND(`privateLayout=0`)

     AND(`friendlyURL='/login'`);
  5. restart web server
  6. Log into OMNM
- **Port Details -** Switch Mode is only populated for devices that support the Bridge-MIBs. The default value is unknown. (27498)
- **Adaptive CLI -** NPE when executing ACLI that is not associated to the device using groups. (27603)
- **Topology Crashes—** Topology crashes at random intervals in Chrome Browsers. This appears to be a stability problem with the internal Pepper Flash player that comes bundled with Chrome. **Workaround:** Download and install an external Flash player. (http://get.adobe.com/flashplayer/)

  Set Chrome to use the external player rather than its internal player.
  1. Type `about:plugins` as a url.
  2. Click on details in the upper right corner.
  3. Scroll through list looking for Adobe Flash Player and disable the internal one and enable (if not already enabled) the external version.
  4. The internal one will be located in a path something like this

     ```
     C:\Program Files(x86)\Google\Chrome\Application\39.0.2171.65\
       PepperFlash\pepflashplayer.dll"
     ```
  5. The external Flash has a path something like this

     ```
     C:\Windows\system32\Macromed\Flash\pepflashplayer32_16_0_0_233.dll
     ```

  (hd-3057)
- **Menus**—If your menu appears vertically, on the left side of the screen, you may have difficulty opening all of the items that appear in it if you move the cursor from top to bottom to open pages and sub-pages. **Workaround**: Move the cursor from bottom to top. (37177)
- **Thread Dumps Impact Disk Space**— Java JVM problems can generate over 10GB of thread dump in case of memory error. **Workaround:** Delete the `*.hprof` files in the `/oware/jboss-5.1/bin` directory to free up the disk space. You can also clean out temp directories. Finally, ensure your hardware has enough RAM for the tasks it was assigned. The Server Statistics portlet displays performance information. (24405)

- **SNMP v3 and Traps**—Traps from an SNMP v3-accessed device do not appear when you change an SNMP v3 login or password on the device or OMNM, unless you resync the device, or until an SNMP monitor polls the device. (23818)
- **IP v6—**Traffic Flow Analysis discards IP v6 packets. You also cannot install to an IP v6 server, and inter-server communications in distributed installations must be IP v4.
- When end user presses on Export button while no data in MIB table, an empty URL comes up. Load Mib table before exporting. (26999)
- **Direct Access** — As of Chrome version 42, 43, and 44, Chrome web browser disables NPAPI as default. This means Direct Access will no longer work on those versions, unless NPAPI is enabled.

  To enable NPAPI in Chrome Version 42, 43, and 44, an additional configuration step is required to continue using NPAPI plugins.

  In your URL bar, enter:

  chrome://flags/#enable-npapi

  Click the Enable link for the Enable NPAPI configuration option.

  Click the Relaunch button that now appears at the bottom of the configuration page.

  As of Chrome 45 (September 2015) Chrome will no longer support the NPAPI plugin. This means java will no longer be supported in the Chrome web browser. The only work around is to use a non chrome browser that supports java.

  This only affects the Direct Access feature used to invoke a direct session to a target device. (27229)

Install/Upgrade

- Permission Updates - After upgrade to OMNM 6.1, you may see a message in Configuration Files portlet that says you do not have permission to view this application. This updated permission permits no access by default and needs to be reset by user. To see or alter them, any administrator user can look in the Permissions in Control panel.

  Go to > Control Panel > Permission Manager > Edit Administrator role > click Add > select 'Configure Files' from the Select Permission list > Check all the check boxes > click Apply > Click Save

  Finally, you must also log out and log back in for any permission change to take effect. (23888)
- When upgrading, you must delete the *Dell PCT Set SNMP User Name* and *Dell PCT L3 Set CoS Interface Settings* Adaptive CLIs to avoid duplicates when upgrading to v6.0. (24932)
- Allowed Negative and special characters for Initial Size and Max Size fields during HA install. (27513)
- Validation is not provided for Config Server IP field during OMNM 6.1 installation. (27456)

- Migration or upgrade from the OMNM standalone/single server environment to a HA environment is not support. Migration or upgrade from an HA environment to a standalone/single server environment is also not supported. User is expected to uninstall and re-install the target platform in these cases (27502)
- Installation scans the following ports:

  Database: 3306 or user-configured database host, if using MySQL server.

  Application server: 8089, 8162, 8489 [HTTPS], 8082

  Web Portal: 8080

  TCP: 161, 162

  Syslog: 514

  When installation encounters a conflict with any of the above ports, a panel appears displaying a warning and the ports in conflict. If your installation has no port conflicts, then no panel appears. (22209)
- MySQL Setup window erroneously allows alphabetical characters in *Initial Size* and *Max Size* fields in the MySQL Setup window. (26938}
- The installation wizard controls the presence of its console. To see the console's contents, look in the installation's target directory for `install.log`. (25712)
- You can upgrade to this release only from OMNM 5.0 or later. Upgrades from previous versions of OMNM are not supported.
  —If you upgrade from 5.0, you must re-register any additional licenses you have purchased by opening the Settings > Permissions > Register Licenses menu, and locating the license upgrades for what you have installed previously.
- If you upgrade from packages that install to a different path from the default (for example OMNM 5.3) to OpsCenter, you may encounter the following problems:
  - The shortcuts in Windows Program menu all point to c:\Dorado rather than the package's path (for example: C:\Program Files\Dell\OpenManage\Network Manager\oware\synergy\tomcat-7.0.40\bin\startsynergy.cmd).
  - Windows also tries to retrieve the shortcut icons from c:\Dorado. **Workaround:** Right-click the shortcut and enter the correct path to the application and/or icon.
  - After upgrading, permissions for the Configuration File portlet need to be reset. **Workaround:** Grant permissions for roles in Control Panel's Permission Manager (23712)
- The first time you start the application after you install it, you may have to wait an additional five minutes for Application to completely start. One indication you have started too soon is that the Quick Navigation portlet does not appear properly. **Workaround:** Force OMNM to re-initialize the admin user. To do that: Login as Admin. Go To > Control Panel > Users and Organizations. Select and edit the Admin user. Edit any field (Middle Name for example). Save. Signout. Log back in with admin. (hd-2259)
- After upgrade, now supported, but previously unsupported devices may appear with their vendor designated as 6027 (in other words: unknown). **Workaround:** Follow these steps:
  1. In web client remove the device(s) in the Managed Resources portlet (right click, then select *Delete*)
  2. Rediscover the device(s) (26569)

- **Ethernet Link Discovery Limitation**—For all Force10 devices, Dell OpenManage Network Manager does not discover ethernet links when they are attached to management port because the LLDP table on the device is not populated. (20579)
- **Server Start Delay—**The Windows tray icon may prematurely indicate application server has started. **Workaround:** Wait for five minutes, and the application server should start completely with the proper icon shown. (18778)
- **Virus Warnings**—Two files installed with this product—`bash.exe` or `md5sum.exe`—may trigger warnings with some anti-virus software. If you get a virus detection warning for these files during installation, take no action. You may want to turn off virus detection while installing.
- **Installing on Windows 2012** must be in compatibility mode. Right-click the `win_install.exe` file (not the shortcut, but the file in the `NM` directory under the installation source directory), and select the Compatibility tab. Check Run this program in compatibility mode for ... then select either Windows 7 or Vista. Command line installations are supported without any compatibility issues. (22634)
- Microsoft Windows 2008 Terminal Server is not supported. The installer becomes non-responsive with Data Execution Prevention enabled. This option is disabled by default on Windows Server 2008, but is enabled on a Windows Server 2008 machine running Terminal Server. (2310)
- Uninstalling sometimes does not delete files in use. Examples can include the following:
  - Uninstalling can leave behind a folder or file in the installation director that was open.
  - If an oware prompt in a command shell is running the oware3rd directory can remain after restart.
  - If your system is slow to shutdown and release the Synergy or Oware services, the oware/synergy or oware folder can remain after uninstall.
  - The uninstaller itself is slow to shutdown and release its own resources. This can result in the jre folder or the Uninstaller folder remaining after uninstall. (23146)
- The traffic flow analysis display does not wrap the names of devices listed in the flow chart, so a published pdf of the chart may cut off names. (26545)
- The Adaptive CLI editor does not apply changes made to all its tabs (Script Content, Continue Pattern, Error Pattern and Value Extraction) when you click *Apply*. The *Close* button may still erroneously apply changes in other than *Script* content tab. **Workaround:** Delete any erroneously saved change, re-make the Error Pattern or other changed tab, Apply changes for each tab, one at a time. Then save the Adaptive CLI from the script edit screen. (hd-2919)
- Network Dashboard portlet fails after the discovery of a WMI device. **Workaround:** Restart application and/or web server. **Fixed:** Release 7.2.3. (25923)
- Converged ethernet switches do not display their equipment type information in network view (Topology) and the icon is different. **Workaround:** This information appears in the Details panel. (24600)
- You cannot filter port-based Adaptive CLIs based on device attributes like *Vendor*. This means selecting *Actions* for a Force10 device port may display other vendors' Adaptive CLIs (24332)

- OMNM does not support Traffic flow analysis on sFlows from devices using sFlow earlier than v5. Typical error content reads “Data array too short“ if you have an unsupported sFlow version. (25134)
- OMNM now shows the top N exporters if it finds no traffic flow data for a selected resource in the selected time frame. (22335)
- To see if a device is registered to display traffic flow in the Managed Resources portlet, you must expand the portlet. You can then display the *Registered* column in the portlet configuration menu (the wrench). (25101)
- The *Freeform* page layout may not work correctly, or may stack portlets on top of one another. **Workaround:** Best practice is not to use it. (25111)
- Limit monitor targets to 10,000 or less per monitor. The *User Guide* also offers suggestions about how to manage such limitations. (hd-1940)
- With SSL enabled, Firefox (v23.0.1) and Flash (v11.8) do not allow monitor importing to work. **Workaround:** Use Chrome. (23671)
- **Java Security and Direct Access**—Some Java installations may block self-signed websites, interfering with Direct Access. The workaround is to provide a security exception for the application server, as follows: (24736)
  1. Click Start
  2. Type `configure java` and hit [Enter]
  3. Select the *Security* tab.
  4. Click *Edit Site List*
  5. Click *Add*
  6. Type the Dell OpenManage Network Manager URL (example: http://192.168.0.51:8080/
  7. Click *OK* and *Continue.*
  8. *Apply* this change, and/or click *OK.*
- If *Max Items per Page* in portlet displays does not retain your settings, it may require second attempt. (24786)
- Saving topology views works on Safari browsers version 6 +, but not older versions (16336)
- When attempting to access a device configured with SNMP v3, if you see an error message like “unable to read device serial number for selected credential,“ discovery or other access fails. **Workaround:** This indicates the SNMP v3 credential is faulty. Correct it, and discovery and access should be available. (19172)
- Dell OpenManage Network Manager Traffic flow analyzes only IP-type traffic. Consequentely the following parse errors can appear in the application server log for some flow data.

  `Parse error: Unable to process non IP type flow. Type: <Number>`

  <Number> represents an Sflow packet type. This application only parses data of type IP. When Dell OpenManage Network Manager receives non-IP packets, it drops packets and this error appears. (23218)
- You can safely ignore a Solaris shell message saying `solaris_install.bin` not found. (19108)

- After upgrading, Users may not initially appear associated to their roles, but you can work around this apparent failure by clicking *Update Associations*. This is in the Roles portion of the Control Panel. *Click Actions* > *Assign Members*, then click the *Update Associations* button on the following screen. Alternatively, you can go to the Server Administration portion of the Control Panel and click *Execute* to Reindex all search indexes. (19876)
- If a problem occurs during firmware deployment, the error message displayed may not specify the cause. Failed connectivity may produce a message like "Error pattern '.*(is required ' matched 'already full'" **Workaround:** For such messages, the content of the error message, visible at the bottom of the audit screen, may provide more information. Click the message in the top of the audit screen to read its contents in the bottom of the screen. (18636)
- The Organization User in Roles has no description. Its features are covered in the online help and User Guide. (18669)

Web Client

- Screen resolution must equal or exceed 1280 x 1024 pixels. Your screen must be at least 1250 pixels wide. Even in these circumstances, some cosmetic aberrations may occur (duplicate forms for one example). You can safely ignore such aberrations. (25085)
- Audit Trail may show blanks for the Subject column in the Audit Trail portlet. This is because some audited tasks are targetless. (17643)
- Exporting to Excel does not work in Internet Explorer. **Workaround:** Ctrl + click the Excel export button in Dell OpenManage Network Manager. (13456)
- Mutlitab browsing is not supported and may produce unpredictable results. (10963)
- In a job viewer window, some audit trail messages may appear too narrow to read in their entirety. **Workaround**: Maximize the browser and you should see the message details in the expanded job viewer window. (16320)
- In some cases a single managed object may be discoverable via multiple IP addresses. Each discovered IP creates a new inventory object and will count against any licensed Right To Manage total. **Workaround:** Network elements should be managed through a single interface/IP. Additional discovered interfaces should be deleted leaving only one managed object in inventory. (11540)
- Link discovery currently does not find one-ended links. (16305)

- Devices not implementing LLDP MIBs with complete and correct data will prevent OMNM from discovering links for the device. Also some devices encode STP data collected via SNMP in a way that is difficult to decipher. In these cases, Dell OpenManage Network Manager logs a warning message `Problem determining designated port encoding algorithm` during device link discovery. (16438)
- A device login banner can not contain the same character(s) that are used during the device login sequence. For example hashmarks (#) greater than symbols (>) etc. (24992)
- Due to a bug in the implementation of a card-marking performance optimization in the JVM (version 6u18), Synergy can crash under heavy load caused by heap corruption.

  To avoid this issue, users should disable card-marking performance optimization:

  For Windows

  1. Edit setenv.bat file located in `...\oware\synergy\tomcat-xx\bin`
  2. Add -XX:-ReduceInitialCardMarks as one of JAVA_OPTS variables

     set "JAVA_OPTS=%JAVA_OPTS% -XX:-ReduceInitialCardMarks -XX:NewSize=%PORTAL_GC_NEWSIZE%....
  3. In Oware environment, navigate to `...\oware\synergy\tomcat-xx\bin` directory and execute service.bat update

     >oware

     $service.bat update
  4. Restart Synergy

  For Linux

  1. Edit setenv.sh file located in `.../oware/synergy/tomcat-xx/bin`
  2. Add -XX:-ReduceInitialCardMarks as one of JAVA_OPTS variables

     JAVA_OPTS="$JAVA_OPTS -XX:-ReduceInitialCardMarks -XX:NewSize=PORTAL_GC_NEWSIZE....
- Restart Synergy.

Configuration Management

- When a device does not support the selected backup protocol, or if no file server is available for the selected protocol, OMNM uses the most secure backup protocol possible given those constraints. This behaviour is works as designed. However, no message appears in the audit trail to indicate that the default was chosen over the selected, but unavailable, protocol (25848)
- Dell Powerconnect devices do not support FTP for backup. If you select FTP, OMNM defaults to the most secure protocol possible (SFTP). (25918)

Event Management

- Starting with v.5.3, ICMP Monitor includes Force10 devices responding to ping.

Reports

- OMNM does not generate a report when the associated template includes too many available columns for PDF to handle (24837)
- Some reports or templates may appear pre-seeded that are not supported by OMNM. For example, pool report templates may appear for programmatic restrictions on pooled assets like IP addresses, or Route Targets that may not be supported. (18882)
- Report icon is cut off using chrome version 42. This is working fine when using chrome version 41. (27221)
- Sometimes it returns data points in the middle of the month. If you are reporting on monthly data then it should only have one data point per month for each entity and attribute. It only does this if you add targets in the middle of the month. Also the code looks like it is averaging averages, which is mathematically inaccurate. It should instead add up all the values and divide by the total number. (27612)

Supported Aerohive Equipment

The following describes supported Aerohive equipment and its known issues.

- Supported device models include: HiveAP1130, AP121, AP122, AP130, AP141, AP170, AP230, AP245X, AP250, AP330, AP350, AP370, AP390, AP550.
- Supported features include the following: Discovery SNMPv1, SNMPv2, SNMPv3, Telnet, SSH, HTTP; Deep Discovery; Configuration File Backup, Restore, Deploy; Proscan, Change Management; Action/Adaptive CLI; Event Management; Performance Monitors (ICMP, SNMP Interface, SNMP, CPU and memory); Reports; Network Views.

Known Issues

No known issues at this time.

Supported Alcatel Equipment

The following describes supported Alcatel equipment and its known issues.

- Supported device models include: OS6250-24, OS6250-24M, OS6250-24MD, OS6250-8M, OS6250-P24, OS6450-24, OS6450-24L, OS6450-48, OS6450-P10L, OS6450-P24, OS6450-P48, OS6450-P48L, OS6850-24, OS6850-24L, OS6850-24LU, OS6850-24X, OS6850-24XL, OS6850-24XLU, OS6850-48, OS6850-48L, OS6850-48LU, OS6850-48X, OS6850-48XL, OS6850-48XLU, OS6850-P24, OS6850-P24L, OS6850-P24LU, OS6850-P24X, OS6850-P24XL, OS6850-P24XLU, OS6850-P48, OS6850-P48L, OS6850-P48LU, OS6850-P48X, OS6850-P48XL, OS6850-P48XLU, OS6850-U24, OS6850-U24X, OS6850E-P48, OS6850E-P48X, OS6850E-U24X, OS9600, OS9600-CMM, OS9600E, OS9700, OS9700-CMM, OS9700E, OS9800, OS9800-CMM, OS9800E.
- Supported features include the following: Discovery SNMPv1, SNMPv2, SNMPv3, SSHv2, HTTP; Deep Discovery; Link Discovery; Configuration File Backup, Restore, Deploy; Proscan, Change Management; Action/Adaptive CLI; Event Management; Performance Monitors (ICMP, SNMP Interface, SNMP); Reports; Network Views.

Known Issues

- OMNM does not support telnet for alcatel devices. The alternative is to use SSH. (28836)

Supported Brocade/Brocade RX Equipment

The following describes supported Brocade equipment and its known issues.

- Supported devices include the following: 6510, AP7600, Connectrix ED-480000B, DCX4S, Silkworm 2800, Silkworm 4100, B-DC 4XS and B-80, B-MLXe4, B-MLXe8, B-MLXe16, B-FCOE1024, B-FCX624, B-FCX624S, B-FCX648, B-FCX648S, B-TI24X, B-RX4, B-RX8, B-RX16, B-8000/8000e, B-DCX4S, M8428k.
- Supportded firmware versions: 5.2.0 or higher.
- Supported features include the following: Discovery SNMPv1, SNMPv2, SNMPv3, Telnet, SSHv2; Deep Discovery; Configuration File Backup, Restore; Proscan, Change Management; Action/Adaptive CLI; Direct Access; Event Management; Fault Management, Performance Monitors (ICMP, SNMP Interface, SNMP); Reports; Network Views.

Known Issues

- If you upgrade to OMNM, fabric information does not appear for some devices. **Workaround:** Delete and rediscover the device after upgrading. (25280)
- OMNM does not discover the management port on Brocade devices. (25024)
- Ports are listed in Brocade's MIBs as ethernet, so OMNM always discovers them as ethernet. (24982)
- M8428K does not display performance indicators in the details panel. (17447)
- A limited amount of interface data is collected from Brocade Ethernet capable switches. As a result, interface reports and the Interfaces portlet do not contain Ethernet Link data.(18800, 18802)
- Right-click menu in Performance - Top Ping Response portlet does not appear. **Workaround:** Right-click in the Managed Resources portlet. (18827)
- OMNM will not telnet connect to some devices if they use the factory default password. You must set the password to something other than that default. OMNM does not recognize the additional prompt asking that default password be changed each time log in occurs. (12240)

Supported Cisco Equipment

The following describes supported Cisco equipment and its known issues.

- Driver support added for Cisco 2960X-24TS-L. (32118)
- The following monitors were added: Cisco Ethernet SLA, Cisco IP SLA, Cisco QOS. (28136)
- Driver support added for Cisco SFP DOM pluggable transceiver components, including Key Metrics monitoring. (24640)
- Driver support added for Cisco ASR 1000 series devices running IOS XE v. 15.x. Devices supported: ASR 1001,1002, ASR 1002F, ASR 1004, ASR 1006, ASR 1013, CSR 1000V (Virtual Emulator). (19509)

- Driver support added for Cisco SFTP, IE-30004-TC, IE-30008-TC, ASR 1002-X, 3850-48P-S. (24682, 2871)
- New Cisco Metro Ethernet SLA Monitor (24633)
- Cisco devices running IOS or IOS-XR can calculate bandwidth. Consult the Monitoring Chapter of the *User Guide* for details. (24997)
- Added support for the following devices: Catalyst 4500 L3 Switch, Catalyst 6500, CBS31X0, C1900, Catalyst WS-C4948-10GE, Router 3600, Router 3800, Router 3900, Nexus 3064, Nexus 5548, Nexus 6506, 6509, 6513, Nexus 7000, 7010, 7018,(24682, 23808, 24012)
- In configuration management, OMNM uses either SCP or SFTP depending on which one is supported. If both are supported, whichever it finds first. If you select *Default* as the Transfer Protocol, OMNM chooses in order of higher priority: SCP/SFTP > FTP > TFTP. (24682)
- Cisco IPSLA Monitor provides end-to-end service verification. Alarms appear in the Service Details Panel and service topology. (18423)
- Support for second generation Cisco devices, including 1921. (19665)
- Discovery—Dell OpenManage Network Manager must be authorized to set CLI session parameters; permissions-related timeouts may occur during device access if it is not. For example, Cisco CLI access requires the command `set terminal length 0`. (20679)
- Cisco IOS-based devices now support web interfaces for backup, restore, deploy and direct access. OMNM no longer has an option to restore running or startup configurations. Such devices always restore to the running configuration, then copy to startup for IOS versions below 12.4. For versions 12.4 and greater, devices no longer merge, but use the `configure replace` command to restore the new config file cleanly then copy to startup. (14004)

Known Issues

- OMNM **does not** currently support deployment of Cisco Nexus devices. (30812)
- Initial discovery of Cisco XR devices could fail while configuring the SNMP trap settings on the device. This could be because the application couldn't login to the devices as the number of cli sessions to the device was maxed out. If this happens, the snmp trap setting can be done by running the snmp task from the actions portlet against the xr device. (29389)
- Nexus configuration restore to start-up is not supported. When you attempt this, an error including `This command is deprecated` appears on 3000 series devices. On 5000 series, the error is `sysmgr_copy_nvram_dest_action: src uri_type = 1 is not supported yet`. (25242)
- An Adaptive CLI whose script is `show protocols` fails for devices with IOS 12.4(9)T7 firmware. No such issue exists in the newest version of IOS 12.4T which is 12.4(24)T. `Workaround:` Update the device's firmware. (23132)
- LLDP link discovery on switches running old versions of Cisco IOS 12.2 (pre-55 revision) not supported. **Workarounds:** Upgrade the IOS version. Alternatively, enable CDP and find the link using CDP instead. (16468)
- OMNM only supports Cisco router to router, or router to switch ethernet link discovery when the CDP is turned on for ports on each end. For other vendors, you must have LLDP active, or ethernet link discovery is not supported. (16261)
- Cisco Firewall Services do not backup, restore, deploy and Direct Access. (15765)

Issues Resolved

No resolved issues to report/

Supported Cisco LAN Switches Small Business Equipment

The following describes supported Cumulus equipment and its known issues.

- Supported devices include:

  SF 200-24, SF 200-24FP, SF 200-24P, SF 200-48, SF 200-48P:

  SF 300-08, SF 300-10, SF 300-10MP, SF 300-10P, SF 300-20, SF 300-24, SF 300-24P, SF 300-28, SF 300-28P, SF 300-48, SF 300-48P, SF 300-52:

  SF 302-08, SF 302-08MP, SF 302-08P.

  SF 500-24, SF 500-24P, SF 500-48, SF 500-48P;

  SG 500-28, SG 500-28P, SG 500-52, SG 500-52P;

  SG 500X-24, SG 500X-24P, SG 500X-48, SG 500X-48P.
- Support SX300 firmware 1.4.x.
- Supported features include the following: Discovery SNMPv1, SNMPv2, SNMPv3, Telnet, SSHv2, HTTP; Deep Discovery; Link Discovery; Configuration File Backup, Restore, Deploy; Proscan, Change Management; Action/Adaptive CLI; Direct Access; Event Management; Performance Monitors (ICMP, SNMP Interface, SNMP); Reports; Network Views.

Known Issues

- Memory and temperature are not supported by device.(27637)

Supported Cumulus Equipment

The following describes supported Cumulus equipment and its known issues.

- The supported version of Cumulus Linux is 2.5. support any model that run Cumulus Linux.
- Supported features include the following:
  - Device Discovery.
  - LLDP Link Discovery.
  - Configuration File Backup/Restore.
  - Reporting for any data/attributes collected. Inventory/Asset etc.
  - Command line access.
  - Actions (these are pre-seeded or user defined scripts that can be executed against devices).
  - Proscan.
  - Configuration Change and compliance management
  - Performance Monitoring (ICMP, SNMP, Memory and CPU ultilization).
  - Topology.

NOTE:

The device needs to have these settings for snmp oids to return the right values for cpu and memory. (27489)

https://support.cumulusnetworks.com/hc/en-us/articles/203922988-Exposing-CPU-and-Memory-Information-via-SNMP

Known Issues

- OMNM does not support Cumulus Linux device discovery using root user as CLI authentication. (27289)
- Non-root user must be in the sudoers list (27289)

  To add a user to sudoers list:

  login as root and type 'visudo' to edit /etc/sudoers.tmp file

  Under the line:

  root ALL=(ALL) ALL

  Add the following (replacing user with your username):

  user ALL=(ALL) ALL

  Ctrl+X and press Y when to save and exit

Supported Dell Equipment

The following describes supported Dell equipment and its known issues.

6.5

- Added 6.4 firmware support for Dell Networking N1xxx, N2xxx, N3xxx, N4xxx models. (30171)
- Dell Networking PCT and FTOS drivers support PVID. (29211)
- Driver support added for Dell EMC Networking models N11XX, N2128PX, N3132PX. (28613).

6.2 Service Pack 3

- Added 9.11 firmware support for Dell Networking FTOS models: S6100, S6010, S4048T-ON, S3100, S3148, S3124, S3124F, S3124P, S3148P, IOA/MXL, FX2 IOA, S4810, S4820T, S5000, S6000, Z9500. (28755)
- Driver support added for Dell Networking N3132PX model running 6.3.5.x firmware. (28768)

6.2 Service Pack 2

- Added 6.3.0.19 firmware support for Dell Networking N1xxx, N2xxx, N3xxx, N4xxx models. (28389)

6.2 Service Pack 1

- Driver support added for Dell Networking FTOS models: S6010, S4048T-ON. (27836) (27838)
- Added 9.10 firmware support for Dell Networking FTOS models: S6100, S6010, S4048T-ON, S3100, S3148, S3124, S3124F, S3124P, S3148P, IOA/MXL, FX2 IOA, S4810, S4820T, S5000, S6000, Z9500. (27757) (28042) (27909)

- Added firmware 3.0.0.70 support for Dell Networking X-1000 Series switches. (28043)
- Devices running 9.10 firmware version or newer are collecting KPI information using SNMP protocol. Since older firmware doesn't support KPI information using SNMP protocol, OMNM still needs to use CLI to retrieve information from the devices. (27757)

6.2

- Driver support added for Dell Networking W-series : W-7205, W-7024, W-7240XM, W-IAP277, W-IAP228, W-IAP205H, W-IAP324, W-IAP325, W-AP228, W-AP205, W-AP324, W-AP325, W-AP277 (27756)
- Driver support added for Dell Networking FTOS models: S6100, S3100. (27754) (27755)
- Z9100-ON support for Dell FTOS 9.8. Cumulus linux not supported. (27752)

6.1

- Driver support added for Dell Networking X-series switches: X1008, X1008P, X1018, X1018P, X1026, X1026P, X1052, X1052P, X4012.
- Driver support added for Dell Networking model: PowerEdge VRTX 10Gb.
- Fiber Channel Port Statistics information can be obtained using the “Dell Networking (FTOS) Show Interfaces” ACLI. Please specify the fiberchannel interface as the interface parameter. (27148)

6.0 Service Pack 3

- Driver support added for Dell Networking models: N1524, N1524P, N1548, N1548P.
- Added 9.8 firmware support for Dell Networking FTOS models: IOA/MXL, S4810, S4820, S5000, S6000, Z9500, FN 410S/410T, FN 2210S, S3048 ON, S4048 ON.

6.0 Service Pack 2

- Driver support added for Wireless Controllers: W-7005, W-7010, W-7030.
- Driver support added for Instant Access Points: W-IAP103, W-IAP204, W-IAP205, W-IAP214, W-IAP215, W-IAP224, W-IAP274, W-IAP275.
- Driver support added for Access Points W-AP103, W-AP103H, WAP204, W-AP205, W-AP214, W-AP215, W-AP224, W-AP225, W-AP274, W-AP275.
- Added 6.3.1.8 firmware support for wireless Instant Access Point devices.
- Added 6.4.2.4 firmware support for wireless controller devices.
- Added support for Dell Networking FTOS models Z9500, FN410S, FN410T, FN2210S.
- Added 9.7 firmware support for the following devices S4810, S4820,S5000, S6000, MXL, IOA, Z9000, Z9500, FN410S, FN410T, FN2210S.
- Added 6.2 firmware support for Dell Networking models: N2024, N2024P, N2048, N2048P, N3024, N3024F, N3024P, N3048, N3048P, N4032, N4032F, N4064, N4064F..

6.0 Service Pack 1

- Added support for FTOS 9.4, 9.5 and 9.6 firmware.

  Important: If you upgrade OMNM to support these firmware versions, the upgrade also includes a device name change from *Force10* to *Dell Networking*. The

Changes: below outline the changes for devices using firmware 9.4 and later. You may also have to perform manual tasks after upgrade. These are described below. If you are installing this version fresh (non upgrade) you can ignore these *Changes*.

Changes:

- Device models change from name *Dell FTOS <model name>* to *Dell Networking <model name>*
- OS images change from *Dell Force10* to *Dell FTOS*
- Because of the name change, some groups and filters in previous packages will not be fully functional for devices on 9.4 or later firmware. To resolve this, the upgrade adds new groups to pick up both the pre 9.4 and post 9.4 firmware.

These group changes are mapped old to new. (These are in the Group Manager Portlet)

OLD	NEW
Dell Force10 Devices	Dell Networking C/E/M/S/Z Series
Dell Force10 C-Series	Dell Networking C Series
Dell Force10 E-Series	Dell Networking E Series
Dell Force10 M-Series	Dell Networking M Series
Dell Force10 S-Series	Dell Networking S Series
Dell Force10 Z-Series	Dell Networking Z Series

- This change impacts one seeded filter in the Filter Manager: The *Dell Force10 Devices* filter is now *Dell Networking C/E/M/S/Z Series*
- The legacy groups still exist after upgrade. By default OMNM does not preset any objects with these dynamic groups, old or new. You must manually update any OMNM features using the old dynamic group. You need to change this group manually only where a Dynamic group is a filter criterion. If you have not used dynamic groups or if you have already corrected for the new groups, best practice is to delete all of the old groups noted above.

The Reports portlet contains a good example. If you edit the *Inventory Asset Report*, a Resource Groups section appears at the bottom. If you click add you will see variety of Dynamic groups you can add to limit the scope of the asset report. Other options to add dynamic groups appear if you click the Filter tab at the top.

Other Applications allowing dynamic groups appear listed below. Any User-defined dynamic groups must be updated.

Resource Manager

Container manager

Proscan

Performance monitors – You must update monitor options for each monitor if you use user-defined dynamic groups before updating your software.

Performance Monitor Changes:

Product name changes required the monitors change. The monitors now have names starting with *Dell FTOS...* and pick up F10 and Dell FTOS devices for any current F10 monitor, as specified below.

OLD	NEW
Dell Force10 Interface Attributes	Dell FTOS Interface Attributes
Dell Force10 Interface HC Attributes	Dell FTOS Interface HC Attributes
Dell Force10 RMONEtherStatsAttributes	Dell FTOS RMONEtherStatsAttributes
Dell Force10 RMONEtherStatsHCAttributes	Dell FTOS RMONEtherStatsHCAttributes

NOTE:

When you upgrade device from FTOS 9.3, you must resync the device before attempting other functions. ***Also:*** *If any event processing rule (EPR) relies on the device name in the varbind of, for example, a threshold crossing notification, you must accommodate the name change in such rules.*

Previous Versions

- KPI collection now supports decimals, not just integers. (22339)
- Resource Manager now displays the device's MAC address for Dell Networking (PCT) and Dell Networking (FTOS) devices (23803)
- Devices previously displayed as PowerConnect and Force10 now appear as Dell devices. (23804)
- OS Images for Dell Networking FTOS devices with firmware versions 9.4 or later can now store and deploy either Boot Image or System Image or both. If the Boot image is not updated, then you only need to deploy the System Image. To store two files in an OS Image, Ctrl+click to multi-select the files when creating a new image in your database. (26469)
- Support for 9.4, 9.5, 9.6 firmware versions for Dell Networking FTOS devices S4810, S4820, S6000, S5000, Z9000, IOA and MXL models. (26478).
- Upgrade installations remove previously seeded firmware, replacing it with the most current firmware for devices (21952)

Supported Dell EMC Networking PCT Devices

Supported Dell Networking PCT Devices include (brackets enclose reference numbers):

Platform	Supported Firmware Revisions
3524, 3524P, 3548, 3548	2.0.0.x [23795]
5448, 5524, 5524P, 5548, 5548P	4.0.0.x, 4.0.1.x, 4.1.0.x [23794]
6224, 6224F, 6224P, 6248, 6248P	2.1.1.x, 2.2.0.x, 3.2.0.x, 3.2.1.x, 3.3.1.x, 3.3.2.x, 3.3.3.x, 3.3.6.x, 3.3.8.x
7024, 7024F, 7024P, 7048, 7048P, 7048F, 8024, 8024F	4.1.1.x, 4.2.0.x, 4.2.1.x, 4.2.2.x, 5.0.0.x, 5.1.x, 5.1.2.x [24126]
8132, 8132F, 8164, 8164F	5.0.0.x, 5.1.x
M8024, M6348, M8024-K	4.2.1.3, 4.2.0.4, 5.1.x, 5.1.2.x [24126]
M6220	2.2.0.x, 3.1.2.x, 3.1.5.x, 3.3.8.x, 4.2.0.x, 4.2.1.x, 4.2.2.x, 5.0.0.x, 5.1.x, 5.1.2.x [24126]

N1108P-ON, N1108T-ON, N1124P-ON, N1124T-ON, N1148P-ON, N1148T-ON, N1524, N1524P, N1548, N1548P, N2024, N2024P, N2048, N2048P, N2128PX-ON, N3024, N3024F, N3024P, N3048, N3048-EP, N3048P, N3132PX, N4032, N4032F, N4064, N4064F	6.0.1.3, 6.1.0.1, 6.2, 6.3 and 6.4 (OMNM labels 81xx devices as N-Series devices when they upgrade to this firmware. These become N4032, N4032F, N4064, and N4064F models in inventory) [26826]
PowerEdge VRTX 10Gb, PowerEdge VRTX 1Gb IOM	2.0.x
X1008, X1008P, X1018, X1018P, X1026, X1026P, X1052, X1052P, X4012	3.0.x

- Dell has discontinued support for the PC3024, PC3048, PC3324, PC3348, PC3248, PC5012, PC5212, and PC5224 models, although OMNM may still discover and manage these.

Supported Dell Wireless Devices

The following models are supported Dell Wireless models:

Platform	Supported Firmware Revisions
Access Point 1200	
Access Point 2E	
Access Point 40	
Access Point 41	
Access Point 50	
Access Point 52	
Access Point 60	
Access Point 61	
Access Point 61a	
Access Point 65	
Access Point 70	
Access Point 80M	
Access Point 80MB	
Access Point 80S	
Access Point 80SB	
Access Point Duo	
Access Point Duo WJ	
Access Point Mw1700	
Access Point WG 102	
Mobility Controller 200	AOS 2.5.x, 3.1.x
Mobility Controller 2400	AOS 2.5.x, 3.1.x
Mobility Controller 2400E	AOS 2.5.x, 3.1.x
Mobility Controller 2424	AOS 2.5.x, 3.1.x
Mobility Controller 5000	AOS 2.5.x, 3.1.x
Mobility Controller 6000	AOS 2.5.x, 3.1.x
Mobility Controller 800	AOS 2.5.x, 3.1.x
Mobility Controller 800E	AOS 2.5.x, 3.1.x

Mobility Controller 804	AOS 2.5.x, 3.1.x
PowerConnect W-3200	AOS 6.0.1.2, 6.0.2.0, 6.0.2.1, 6.1.1.1, 6.1.2.3, 6.1.3.8, 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-3400	AOS 6.0.1.2, 6.0.2.0, 6.0.2.1, 6.1.1.1, 6.1.2.3, 6.1.3.8, 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-3600	AOS 6.0.1.2, 6.0.2.0, 6.0.2.1, 6.1.1.1, 6.1.2.3, 6.1.3.8, 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-6000M3	AOS 6.0.1.2, 6.0.2.0, 6.0.2.1, 6.1.1.1, 6.1.2.3, 6.1.3.8, 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-620	AOS 6.0.1.2, 6.0.2.0, 6.0.2.1, 6.1.1.1, 6.1.2.3, 6.1.3.8, 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-650	AOS 6.0.1.2, 6.0.2.0, 6.0.2.1, 6.1.1.1, 6.1.2.3, 6.1.3.8, 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-651	AOS 6.0.1.2, 6.0.2.0, 6.0.2.1, 6.1.1.1, 6.1.2.3, 6.1.3.8, 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-7005	AOS 6.4.2.4
PowerConnect W-7010	AOS 6.4.2.4
PowerConnect W-7030	AOS 6.4.2.4
PowerConnect W-7210	AOS 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-7220	AOS 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-7240	AOS 6.2.0.3, 6.2.1.1, 6.3.1.1, 6.3.1.2, 6.4.2.4
PowerConnect W-AP103H	
PowerConnect W-AP124	
PowerConnect W-AP125	
PowerConnect W-AP175AC Outdoor (DC)	
PowerConnect W-AP68	
PowerConnect W-AP68P	
PowerConnect W-AP93H	
PowerConnect W-IAP 204	AOS 6.3.1.8
PowerConnect W-IAP 205	AOS 6.3.1.8
PowerConnect W-IAP103	AOS 6.3.1.8
PowerConnect W-IAP104	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0
PowerConnect W-IAP105	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0
PowerConnect W-IAP108	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0
PowerConnect W-IAP109	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0
PowerConnect W-IAP114	AOS 6.3.1.8, 6.3.1.2-4.0.0.4
PowerConnect W-IAP115	AOS 6.3.1.8, 6.3.1.2-4.0.0.4
PowerConnect W-IAP134	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0, 6.1.3.4
PowerConnect W-IAP135	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0, 6.1.3.4
PowerConnect W-IAP155	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0
PowerConnect W-IAP155P	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0
PowerConnect W-IAP175	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0, 6.1.3.4
PowerConnect W-IAP175AC	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0, 6.1.3.4
PowerConnect W-IAP175P	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0, 6.1.3.4
PowerConnect W-IAP214 (11n/11ac)	AOS 6.3.1.8
PowerConnect W-IAP215 (11n/11ac)	AOS 6.3.1.8

PowerConnect W-IAP224 (11ac)	AOS 6.3.1.8
PowerConnect W-IAP225 (11ac)	AOS 6.3.1.8
PowerConnect W-IAP274 (Outdoor/11n/11ac)	AOS 6.3.1.8
PowerConnect W-IAP275 (Outdoor/11n/11ac)	AOS 6.3.1.8
PowerConnect W-IAP3WN	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0, 6.1.3.4
PowerConnect W-IAP3WNP	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0, 6.1.3.4
PowerConnect W-IAP92	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0, 6.1.3.4
PowerConnect W-IAP93	AOS 6.3.1.8, 6.3.1.1, 6.2.1.0, 6.1.3.4
PowerConnect W-RAP2WG	
PowerConnect W-RAP5	
PowerConnect W-RAP5WN	

Supported Dell Networking FTOS Devices

The followings are supported Dell Networking FTOS models:

Platform	Supported Firmware Revisions
ExaScale (E1200i, E600i)	8.4.1.4, 8.4.1.3
TeraScale (E1200i, E1200, E600i, E300)	8.4.2.6, 8.4.2.5
C300, C150	8.4.2.6, 8.4.2.5, 8.4.2.9
C9010	1.0
Z9000, Z9500, Z9100-ON	8.3.11.4, 8.3.11.3, 8.3.11.2, 9.2.x, 9.3.0.x, 9.4, 9.5, 9.6, 9.7, 9.8, 9.10
MXL, IOA	8.3.16.2, 8.3.16.1, 9.2.x, 8.3.16.4, 8.3.17.4, 9.3.0.x, 9.4, 9.5, 9.6, 9.7, 9.8, 9.10
S25. S50, S50N, S50E, S50V, S50N-AC, S2410CP, S2410P, S25N, S25P-AC, S25P-DC, S25V	8, 8.4.2.6, 8.4.2.5
S55	8.3.5.1, 8.3.5.2, 8.3.5.3
S60	8.3.3.7, 8.3.3.6, 8.3.3.9
S3100, S4810	8.3.7.2, 8.3.10.1, 8.3.12.0, 8.3.12.2, 9.1, 9.2.x, 9.3.0.x, 9.4, 9.5, 9.6, 9.7, 9.8, 9.10
S4820T, S4820	8.3.19.0, 9.2.x, 9.3.0.x, 9.4, 9.5, 9.6, 9.7,9.8, 9.10
S5000, S6000, S6100, S6010	9.0.1.0, 9.1.1.x, 9.2, 9.3.0.x , 9.4, 9.5, 9.6, 9.7, 9.8, 9.10
S3048 ON, S4048 ON, S4048T-ON	9.8, 9.10
FN410S, FN410T, FN2210S,	9.7, 9.8

The following are supported Dell Networking FTOS S-Series models supported in a stacking configuration:

- S60, S55, S50N, S50V, S25N, S25P, S25V, S4810, S4820T, S5000.
- Ports for the POE+ card C150/C300 also appear in the ports portlet (23884)

NOTE:

The latest OMNM version supports FTOS 9.4 and later. It discovers Dell Networking FTOS Devices as Dell Networking Devices. The section of this document describing New Features describes the manual procedures required if you upgrade to this version.

Known Issues for Dell Networking PCT, Dell Networking FTOS and Wireless devices

- When deploying to a stacked N-Series, the device reports the following:

  `Stack port errors detected on the following interfaces"`

  This message causes the OMNM deploy process to state that the deploy failed. (30279)

  Workaround: Check the firmware version on the device to see if the upgrade succeeded.

- Dell Networking N Series devices "Firmware deploy" cannot be used to downgrade the firmware from 6.5 to an older firmware image. This requires a special process as outlined in the Dell documentation. (30718)

  `http://www.dell.com/support/home/us/en/04/product-support/product/networking-n2000-series/drivers`

- As a part of firmware deployment on the Dell Networking N Series devices, the firmware and boot code will be upgraded. CPLD update **is not** a part of the deploy process. (30713)
- The stacking ports are not being discovered for N15xx models due to information missing in entPhysicalTable. (27347)
- A duplicate device cannot be detected if they are in the same discovery profile or range of IPs to be discovered. Detecting the duplicate device will only work when one of the devices has already been discovered. (27942)
- X-Series don't support "Boot system image-1" command. As a result, during deployment process, device will reboot from device pre-selected boot image. (27275)
- Poweredge VRTX doesn't support memory KPI. (27430)
- Poweredge VRTX - serial number not discovered. (27432)
- Download firmware for dell powerconnect not functioning remove. (27438)
- Despite job status for Dell Force10 TFTP configuration restores showing success, you may see an Timeout error message. This message can be safely ignored. (27013)
- Because of a firmware bug, Layer 2 PowerConnect switches only support telnet for all CLI based features, not SSH. (hd-2913)
- For Dell Networking FTOS devices with firmware 9.6 installed, resync may display an error on the command `show fc switch`. **Workaround:** With this firmware you must enable the `fc` feature for the `show fc` command to work. Enable that feature and resync works without error. (26481)
- Upgrading from previous versions may produce a seeding error because a report template (Dell S5000 Fabric Device Template) has changed. **Workaround:** Before

upgrading, delete the Dell S5000 Fabric Device Template in the Reports Template and delete that report in the reports portlet.

- Restoring configurations with the startup/reboot option works on N Series devices running 6.x firmware, but the audit trail may not indicate the correct status. This occurs because OMNM does not receive anything from the device to close out the job. Some models do not send a message like `Shutting down..` that indicates success.(23976, 23785)
- FTOS Devices do not support the Q-BRIDGE-MIB, and therefore discovery does not find VLANs connected to these devices. (1893)
- You must delete and rediscover Dell Networking FTOS MXL and Dell Networking FTOS IO Aggregator devices after upgrade from any previous version of this software. This requirement originates from a device type change. In previous versions, these devices were switches, but now they are converged ethernet switches. (23970)
- The Adaptive CLI set MSTP global settings does not execute all the commands on 7xxx & M8024K models 5.1 firmware. (21314)
- IPv6 ping and telnet is not supported. (23056)
- Backing up Dell Powerconnect W-Series iAP devices is not supported. (18560)
- MIB browser cannot read some Dell Networking FTOS MIB tables. (23318, 19461)
- During peak traffic times, deploying firmware to Dell Networking FTOS S-Series may fail with the following error messages:

  ```
  sent command 'upgrade system stack-unit all A:'
  matched pattern '% Error:.*'
  on line '% Error: Invalid inut at "^" marker
  ```

  Workaround: If this occurs, retry deploying later, when traffic to/from the device is not high. (23320)
- For PowerConnect devices running 5.x or 3.x firmware, restoring startup config may incorrectly display a timeout error, even if the restore succeeded.

  The reason for this is that Dell OpenManage Network Manager does not get anything from the device to close out the job. Some models do not send a message like `Shutting down..` that indicates success.(22411)
- Executing an Adaptive CLI reload may produce a false failure error message. This occurs because OMNM loses connection and the device does not respond. Device reload is sometimes successful in these circumstances, but must be manually verified. (22453)
- Dell Networking FTOS device discovery fails when its login banner is configured as *Keyboard-interactive* in the DUT. This makes manual interaction with the device necessary, so automated discovery fails. (22768)
- Follow the instructions and minimum requirements documented in the S4810 FTOS version E9.1.0.0 release notes before using OMNM to deploy FTOS version E9.1.0.0 or greater to S4810 devices. S4810 units must not run FTOS version E8.3.12.1 when initiating OMNM discovery or re-sync. If an S4810 unit is running FTOS version E8.3.12.1, then upgrade the device to FTOS version E8.3.12.2 before starting OMNM discovery. (21424)
- PowerConnect 5500 and PowerEdge 1GB VRTX switches do not display memory utilization because the device provides no CLI and SNMP implementation to fetch these values. (21995, 21351)

- FiberChannel ports are excluded from the ALL Devices group for the default interface monitor. Monitors do not retrieve information from FiberChannel ports, so including them would distort monitoring results. (23033)
- Stacking with 35xx series may have timeout issues when trying SNMP get to walk thru all the ports and related details (monitoring). (19394)
- For devices running firmware older than 4.1.x.x, you must use a non-default enable access method or save an enable password in the startup configuration before upgrading to the newer versions to access privileged exec (enable) mode via telnet or SSH after the upgrade. The 4.x.x.x firmware emulates industry standard behavior for privileged exec (enable) mode authentication over SSH and telnet. In 4.1.x.x, the enable authentication method requires a password and the default list for telnet and SSH (enableNetList) contains only the enable method with no password. If the configuration being upgraded does not have an alternative enable authentication method defined (for example TACACS), setting an enable password allows one to access privileged exec mode after the firmware upgrade. (19387, 19512)
- When a device does not have the enable mode enabled, a benign error may appear on login. You can safely ignore this error. (18492)
- Deploying a firmware image on an Access Point is not supported. (18637)
- In the Image Repository portlet, clicking on Download > Firmware for Dell PowerConnect may download out of date firmware for Dell PowerConnect classic devices. **Workaround:** OpenManage Network Manager has the latest firmware pre-seeded for devices and you can download firmware for each device from the Dell support site. (16561)
- Some Dell devices and firmware revisions may not support the collection of Service Tag and Asset Tag by Dell OpenManage Network Manager. This includes recent firmware revisions of PowerConnect B-Series, and W-series along with older revisions of PowerConnect firmware. (16098)
- When ACLs are configured on Dell Networking FTOS S4810 devices, when copying a restored configuration to the running configuration, an error may appear during restoration. (18905)
- For Dell Networking FTOS devices, interfaces like management and loopback may appear as both ports and interfaces. (18309)
- For Dell PowerConnect M8024-k and 8024/F user ports that are used for stacking ports do not appear in the Network View. (16944, 16951)
- 8024/F fibre channel link discovery is not supported. (16943)
- Some devices do not respond to commands unless they are in the correct state. For example, some Dell devices must not be in “Simple” mode to respond to Adaptive CLIs. (17153)
- Some devices, including the Dell Networking FTOS C-Series and E-Series, will allow then drop telnet connections during deployment or file restoration when you select restart as part of the process. This can take from six to eight minutes, though it can take as long as fifteen minutes for a fully populated chassis. During that time, you can ping the device; however, Dell OpenManage Network Manager cannot log in to the device until the reboot is complete. (18277)
- Due to the change made in Model name, the Dell Networking C- Series Devices group filtering criteria no longer shows the correct managed devices in the group. Therefore, before upgrading to OMNM v.6.0 Service Pack 3, you must either

delete the Dell Networking C- Series Devices group in the Managed Resource Groups portlet, or edit the filter criteria to 'Model contains Force10 C OR Model contains Dell Networking C'. (27371)

Issues Resolved

- Dell Networking FTOS S-Series filters pick up any device whose model name contains “S.” **Workaround:** Use the new *Dell Networking S* group. (26445)
- The Interface availability report displays negative values when the device’s availability is indeterminate. (25576)
- No warning/message appears when the license expires (19375)
- Upgraded openSSL to version 1.0.2c that fixes the vulnerability (heartbleed) issue. (2643)
- Device status is flapping from Responding to Indeterminate randomly (18787)
- Network Topology Background Image is not saved as default. (17641)
- Network dashboard does not really provide useful data without displaying to which device the interface belongs. Now you can hover the cursor over a label to see the device name. (14531)
- The Hardware Change report may erroneously display devices that just had a firmware upgrade or downgrade. (19358)
- **Discovery**—When specifying network addresses using the Subnet type, you must specify the Network address at the beginning of the subnet since Dell OpenManage Network Manager assumes it is the starting IP address for the range. If you specify an address in the middle of the subnetwork then Dell OpenManage Network Manager may discover devices outside of that subnetwork. This also means that IP addresses in the network that precede the specified address are not discovered. To avoid these issues, use the CIDR specification of the network to discover rather that the subnet ID. (16803)
- If you de-select ping as part of a discovery profile, discovery fails to validate authentications. (PV-18146)The latest F10 MIBs contain S4820T device in the F10-Products-MIB, however, the F10-Products-MIB used most recently in Dell OpenManage Network Manager does not contain this device, or Z9000, MXL, IOA. (21029)
- Dell Networking FTOS S-Series filters pick up any device whose model name contains “S.” **Workaround:** Use the new *Dell Networking S* group. (26445)
- The Dell Networking FTOS S50AC device appears as a Dell Networking FTOS S50DC device (17890).
- The firmware report displays unnecessary entries showing firmware changes from empty to a firmware number. (18719)
- For Dell Networking FTOS S50V devices Dell OpenManage Network Manager may show total memory to be less than memory used. (18301)
- You must click the drop down combo box for adding a port to a VLAN or adding an interface to port-channel twice to open the box. (19847)
- The Dell Networking FTOS device driver appears as Force 10 FTOS Service Pack 1 in the MIB Browser. (21028)

- Restoring configurations to Dell Networking FTOS devices may produce errors when individual commands already exist in the running config and cannot be overwritten. Dell OpenManage Network Manager ignores such errors and reports success by default since the errors indicate a command was not applied, not that restoration was unsuccessful. Best practice is to restore to startup config to avoid these errors, especially when scheduling backup or backing up a group on such devices. (17991)
- For Dell PowerConnect 8024/F, restoring a configuration for a stack of devices may fail. (16953)
- CPU and Memory usage values do not appear for PC 5524P (17505)
- You cannot deploy 3.3.x firmware to a PC6248 device that is running 3.x firmware. **Workaround:** Manually deploy the firmware. (19236)
- installer need to check for max partition name length (26790)
- Disabling ICMP ping in Discovery Profiles can also disable the Inspect feature. **Workaround:** Enable *ICMP Ping Devices* (as it is by default). (18146)

Supported Edge Core Devices

The following describes supported Edge Core devices and their known issues.

- Supported device models include: ECS4210-12T, ES3510MA.
- Supported features include the following: Discovery SNMPv1, SNMPv2, SNMPv3, Telnet, SSH, HTTP; Deep Discovery; Link Discovery; Configuration File Backup, Restore, Deploy; Proscan, Change Management; Action/Adaptive CLI; Event Management; Performance Monitors (ICMP, SNMP Interface, SNMP, CPU and memory);Traffic Flow Analyzer, Reports; Network Views.

Known Issues

- In configuration backup , if the user picks a protocol that is not supported by the driver , the application uses one of the protocols supported by the driver. The user will not receive an error message saying that the selected protocol is not supported by the driver or that the protocol used for backup will be one of those supported by the driver. (28716)

Supported EMC Unisphere Devices

The following describes supported EMC Unispher devices and their known issues.

- Supported devices include: EMC Unity
- Supported features include the following: WBEM HTTPS; Deep Discovery; Reports; Network Views.

  Device Specific Monitors.

  At Top level : CpuUtilization, MemoryUtilization, MemoryAvailable, MemoryUsed, ISCSIReadBytes, NetworkIn, NetworkOut, LUNAverageRead, LUNAverageWrite, LUNAverageQueueLength, LunReadBytesRate, LUNReadRate, LUNResponseTime, LUNTotalCall, LUNWritten, LUNWrite.

At Port Level: FCReadBytesRate, FCReadRate, FCWriteBytesRate, FCWriteRate, ISCSIReadBytesRate, ISCSIRead, ISCSIWriteBytesRate, ISCSIWriteRate, PacketsNetworkIn, PacketsNetworkOut, OctetsIn, OctetsOut.

At the LUN/Disk level: LUNAverageRead, LUNAverageWrite, LUNAverageQueueLength, LunReadBytesRate, LUNReadRate, LUNResponseTime, LUNTotalCall, LUNWritten, LUNWrite.

Known Issues

No known issues at this time.

Supported HP Procurve Devices

The following describes supported HP Procurve devices and their known issues.

- Support added for STFP. (24683)
- Supported devices include the following:

  A6713A, A6716A, A6717A, J3177A, J3299A, J4110A, J3100A, J3175A, J3245A, J3298A, J4120A, J4121A, J4122A, J4122B, J4138A, J4139A, J4812A, J4813A, J4819A, J4840A, J4841A, J4860A, J4865A, J4874A, J4887A, J4899A, J4899B, J4899C, J4900A, J4900B, J4900C, J4902A, J4903A, J4904A, J4905A, J4906A, J8130A, J8133A, J8153A, J8154A, J8155A, J8164A, J8165A, J8433A, J8474A, J8680A, J8692A, J8693A, J8697A, J8698A, J8718A, J8719A, J8752A, J8753A, J8762A, J8770A, J8771A, J8772A, J8773A, J8992A, J9019A, J9019B, J9020A, J9021A, J9022A, J9028A, J9029A, J9031A, J9032A, J9038A, J9049A, J9050A, J9085A, J9086A, J9088A, J9089A, J9091A, J9138A, J9145A, J9279A, J9280A, J9299A, J9310A, J9311A, J9470A, J9471A, J9477A, J9623A, J9624A, J9625A, J9626A, J9627A, J9727A, J9729A, J9772A, J9773A, J9774A, J9775A, J9776A, J9778A, J9781A, J9782A, Proliant Series Switches.
- Supported features include the following: Discovery SNMPv1, SNMPv2, SNMPv3, Telnet, SSHv2, HTTP; Deep Discovery; Link Discovery; Configuration File Backup, Restore, Deploy; Proscan, Change Management; Action/Adaptive CLI; Direct Access; Event Management; Fault Management, Performance Monitors (ICMP, SNMP Interface, SNMP); Reports; Network Views.

Known Issues

- OMNM may not always detect telnet disconnects sent by a device. A timeout may indicate a false failure for the telnet session when it is actually successful. This means the system may be unable to detect a disconnect has occurred between itself and a device when a device reboot accompanies restore or deploy actions. (4296, 2338, 4323)
- Due to limitation of the switch, we are not supporting temperature. (27574)

Supported Juniper Devices

The following describes supported Juniper devices and their known issues.

- The following monitors were added: Juniper COS, Juniper RPM. (28136)
- Support added for VMX model, except for backup. (24557)
- Support added for HTTP/HTTPS access (24559)
- Supported devices include the following:
  - EX4500
  - EX6210
  - EX82xx
  - EX8208
  - EX8216

NOTE:

Because EX models transmit MAC address but not IP address, OMNM does not support Traffic Flow Analysis for these models.

- Supported devices include MX80 (14703)
- Support added for JunOS 11.2. and 12.x
- A router-advertisement statement now exists for IPv6 interface services. (18797)
- Support added for JunOS 10.4R4.5. (15549)
- Updated user interface

Known Issues

- When editing a Juniper interface service, the physical encapsulation field is blank, even when it has ethernet configuration configured. This is a restriction from the JUNOS devices. This encapsulation type is no longer supported or is undocumented. OMNM does not display undocumented configurations. (22272)
- In a Juniper Interface template, adding a new inet address service template, and attempting to save without setting the address displays an unexpected validation error. **Workaround:** After saving the VRF service template, use the Copy Interface feature to copy an existing interface with an inet address template, save the interface template, then its inet address sub-service saves. (23628)
- In Static Route services, filling in the first Next Hop information does not persist. **Workaround:** Fill this information in twice. (19434)
- Deploying an interface service with a description that contains double quotes (for example “test port”) fails with a syntax error. **Workaround:** Avoid double quotes in interface service description fields. (19508)
- If you encounter a timeout when deploying an OS image, increase the management CLI interface's timeout to a higher number, for example:. 100 seconds. (15859)
- No support in Juniper BX 7000 Gateway for backup, restore, deploy and Direct Access. (15772)

Supported Ruckus Devices

The following describes supported Rucckus devices and their known issues.

Supported Devices and Features

- Supported device models include: Ruckus AP R310, Ruckus Wireless ZD 1200.
- Supported features include the following: Discovery SNMPv2, Telnet, SSH; Deep Discovery; Configuration File Backup, Restore, Deploy; Action/Adaptive CLI; Direct Access, Event Management; Performance Monitors (ICMP, SNMP Interface, SNMP, CPU and memory); Reports; Network Views.

Known Issues

- Direct Access terminal not working when login warning enabled with Ruckus devices. (29983)

Supported SonicWall Devices

The following describes supported SonicWall devices and their known issues.

- Supported devices include the following:
  - Generic SonicWALL, Generic SonicWALL SRA
  - NSA 220, 220 Wireless, 240, 2400, 250M, 250M Wireless, 2600, 3500, 3600, 4500, 4600, 5600, 6600, E5500, E6500, E7500, E8500, E8510
  - SuperMassive 10200, 10400, 10800, 9200, 9400, 9600, 9800
  - TZ 100, 105, 105 Wireless, 190, 200 Wireless, 205, 205 Wireless, 210, 210 Wireless, 215, 215 Wireless, 300, 300 Wireless, 400, 400 Wireless, 500, 500 Wireless, 600
- Supported firmware versions: 5.8 or higher.
- Supported features include the following: Discovery SNMPv1, SNMPv2, SNMPv3, SSHv2, HTTP; Deep Discovery; Configuration File Backup, Deploy; Proscan, Change Management; Action/Adaptive CLI; Direct Access; Event Management; Performance Monitors (ICMP, SNMP Interface, SNMP); Reports; Network Views.
- SonicOS Firmware Version Import/Export Support Matrix

  The following matrix illustrates the supported source and destination versions of SonicOS when importing configuration settings from one appliance to another

SonicOS Configuration Import/Export Support

From \ To	5.8 (Min. 5.8.1.12)	5.9	6.1.1.x	6.1.2.x	6.2
5.8 (Min. 5.8.1.12)	Y	Y	Y	Y	Y
5.9	N	Y	N	N	Y (Min. 5.9.0.4)
6.1.1.x	N	N	Y	Y	Y
6.1.2.x	N	N	Y	Y	Y
6.2	N	N	N	N	Y

If answer is "Y" above, please look in below table for your specific products
If answer is "N" above, this configuration upgrade is not supported

Known Issues

- snmpv3 doesn’t support write feature. (27147)
- OMNM does not support discovery of SonicPoints. (27115)
- IPFIX with extensions flows are not supported. (27173)
- IPFIX flows are not supported. (27162)
- SonicWALL devices don't support temperature. (27167)
- Link Discovery is not supported. SonicWALL devices don't populate LLDP tables. (27166)
- Application doesn't support restore of SonicWALL devices due to device limitation. (26388)
- End user will receive an exception in appserver when s/he selects some SonicWALL MIB tables. This is due that device doesn't provide information. (24069)

Supported Vyatta Devices

The following describes supported Vyatta devices and their known issues.

- Supported devices include Vyatta Firewall 5400.
- Supportded firmware versions: 1.0.x, 6.6.x & 6.7.x.
- Supported features include the following: Discovery SNMPv2, SNMPv3, Resync, SSHv2, Telnet, HTTP; Configuration File Backup, Restore, Deploy; Link Discovery; Adaptive CLI; Traffic Flow Analyzer; Performance Monitoring; Reporting. (27459)

Known Issues

- Device doesn't support temperature. (27284)
- Not picking up correct memory from Vyatta device. (27283)