		n-Command MSP 7.1.3
Release Notes	**Release Date: June 27, 2014**	**Notes Revision: June 27, 2014**

Important Note: Effective with version 6.1.3 n-Command MSP also uses TCP port 8443. If your n-Command server is located behind a firewall TCP port 8443 must be open to ensure proper operation. For a full list of ports that n-Command uses see the n-Command MSP Quick Start Guide

Enhancements

These are features that have been added since the last release

- Added Support in n-Command MSP for NetVanta 6410, 1544P Gen2, 1235P, 1531, 123x Gen3, 4660 & 6360

Resolved Issues

These are issues that have been resolved in this release

- Upgrading firmware on a 3rd Gen Total Access 900 using n-Command MSP may fail intermittently or display incorrect output.
- 3rd Generation Total Access 900 part numbers 4243924F5, 4243908F5, and 4243916F5 were showing up as an "unknown" hardware type in the UI. (You must delete them and re-add them in the new version to resolve)
- Firmware Jobs may show as "Failed" in the Jobs section of the UI though they complete properly.
- Improved security within certain Jboss servlets.
- In some cases, the database may consume all available disk space, preventing n-Command MSP from operating efficiently.
- Users in clustered environments may be logged out of the system after a period of inactivity.
- The time zone setting in the UI will now properly update the system time zone setting.

Errata

These are issues that were reported from the field or discovered during internal testing but were unresolved at the time of this release.

- Setting the SNMP server to use version 3 messaging causes no SNMP messages to be sent.
- In some rare cases, a newly deployed n-Command MSP OVA may not prompt the user for the serial number upon initial login.
- Input strings within a Configuration Template may not allow configuration creation without manually editing all fields.
- Firmware Jobs may intermittently fail due to insufficient space on the AOS device's flash though it has sufficient space.
- When running a device discovery job, the interface list does not display any options.
- Only the "admin" account has permission to change the passwords of other user accounts.
- Sorting the devices list by IP address does not sort in numeric order.
- Depending on the browser window size and number of widgets on the dashboard, a scrollbar may be present in the "Missed Check-In" column of the Device Alerts widget.
- Setting the n-Command MSP UI to use port "0" for HTTP or HTTPs does not properly disable the UI access for that protocol.
- File uploads fail when using HTTPS with Mozilla Firefox or Google Chrome. This affects license certificate uploads, firmware file uploads, and config file uploads (for preinstall config jobs). The workaround is to use Internet Explorer.
- n-Command MSP does not properly support NetVanta 1638 units configured for ActivChassis.
- When removing a cluster, if you navigate away from the Administration Dashboard before the process is complete, the GUI will no longer be reachable.
- If a captured SIP call has no caller ID information, PCASH exports from an AOS device to n-Command MSP will fail.
- If the time does not match on all servers in a cluster, the cluster will be left in an inoperable state.
- It is not possible to save an alert template if there are no pre-existing email groups and a new email group is created at the same time the alert template is created.
- When rebooting the server from the system management dashboard, no indication is presented to the user that the server is rebooting.
- If the device alert settings on a device are updated while the Device Alerts tab on the device details page is open, the updated settings are not reflected until the device details page is closed and reopened.
- On heavily loaded systems, several concurrent UI sessions may result in missed check-ins.
- OpenSSL vulnerability CVE-2014-0224 allows a Man-in-the-middle attack.
- OpenSSL vulnerability CVE-2014-0198 allows a type of Denial of Service attack.
- OpenSSL vulnerability CVE-2014-3470 allows a type of Denial of Service attack.
- OpenSSL vulnerability CVE-2010-5298 allows a type of Denial of Service attack.