



# RELEASE NOTES

nCommand MSP  
version 10.1.1  
April 18, 2018

## Trademarks

Any brand names and product names included in this manual are trademarks, registered trademarks, or trade names of their respective holders.

## To the Holder of the Manual

The contents of this manual are current as of the date of publication. ADTRAN reserves the right to change the contents without prior notice.

In no event will ADTRAN be liable for any special, incidental, or consequential damages or for commercial losses even if ADTRAN has been advised thereof as a result of issue of this publication.

## Toll Fraud Liability

Be advised that certain security risks are inherent in the use of any telecommunications or networking equipment, including but not limited to, toll fraud, Denial of Service (DoS) attacks, loss or theft of data, and the unauthorized or illegal use of said equipment. ADTRAN OFFERS NO WARRANTIES, EITHER

EXPRESSED OR IMPLIED, REGARDING THE PREVENTION, DETECTION, OR DETERRENCE OF TOLL FRAUD, NETWORKING ATTACKS, OR UNAUTHORIZED, ILLEGAL, OR IMPROPER USE OF ADTRAN EQUIPMENT OR SOFTWARE. THEREFORE, ADTRAN IS NOT LIABLE FOR ANY LOSSES OR DAMAGES RESULTING FROM SUCH FRAUD, ATTACK, OR IMPROPER USE, INCLUDING, BUT NOT LIMITED TO, HUMAN AND DATA PRIVACY, INTELLECTUAL PROPERTY, MATERIAL ASSETS, FINANCIAL RESOURCES, LABOR AND LEGAL COSTS.

Ultimately, the responsibility for securing your telecommunication and networking equipment rests with you, and you are encouraged to review documentation regarding available security measures, their configuration and implementation, and to test such features as is necessary for your network.

## ADTRAN Technical Support Community

For information on installing and configuring ADTRAN products, visit the ADTRAN Support Community, <https://supportforums.adtran.com>.



Pre-Sales Technical Support  
(800) 615-1176  
[application.engineer@adtran.com](mailto:application.engineer@adtran.com)

Corporate Office  
901 Explorer Boulevard  
P.O. Box 140000  
Huntsville, AL 35814-4000  
Phone: (256) 963-8000  
[www.adtran.com](http://www.adtran.com)

Post-Sales Technical Support  
(888) 423-8726  
[support.adtran.com](http://support.adtran.com)

Copyright © 2018 ADTRAN, Inc.  
All Rights Reserved.

## Contents

<i>Introduction</i> .....	4
<i>Unsupported Platforms</i> .....	4
<i>Supported Upgrade Path</i> .....	4
<i>Features</i> .....	5
<i>Fixes</i> .....	5
<i>Errata</i> .....	5

## Introduction

The nCommand MSP 10.1.1 release addresses customer issues that were uncovered in previous code releases and includes several new features.

This release is generally available code. Results obtained during internal testing have been evaluated and the code has been determined to be ready for general availability. Caveats discovered during testing but not addressed in this build are listed in [Errata on page 5](#).

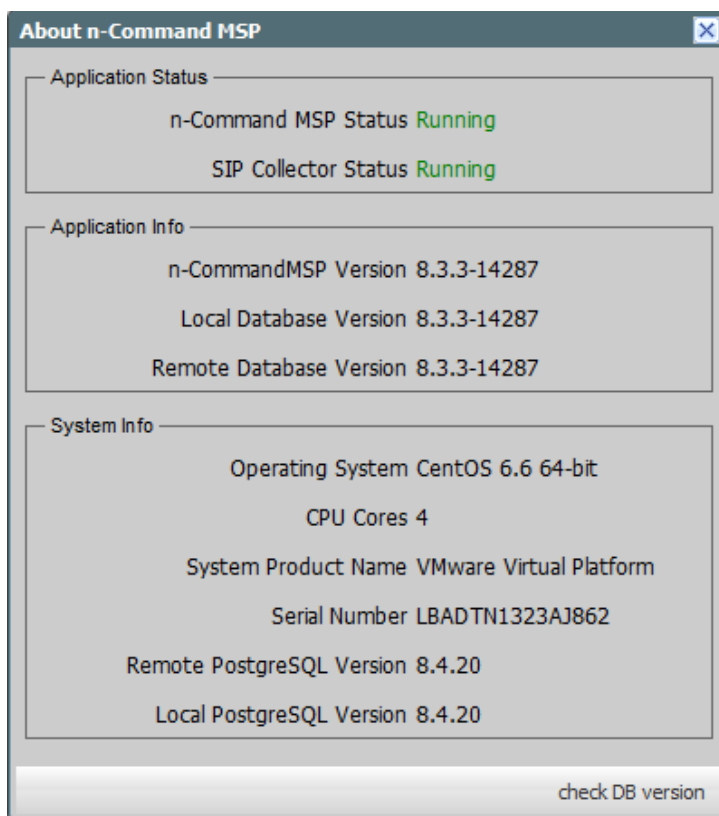
Documentation can be found on ADTRAN's Support Forum, <https://supportforums.adtran.com>, as well as in the in-product accessible online help.

## Unsupported Platforms

The NetVanta 450 n-Command Hardware Appliance is not supported in version 10.1.1. The highest supported version for that hardware is version 8.3.3.

## Supported Upgrade Path

Only servers running host Operating System CentOS 5.6 and above can properly upgrade to version 10.1.1. If your server is running CentOS version 5.5 or below, please contact ADTRAN Product Support at [www.adtran.com/openacase](http://www.adtran.com/openacase) for assistance with your upgrade. To check the current CentOS version on n-Command, log into the admin dashboard at **http:<IP address or hostname of server>/msp**. Navigate to **Help->About n-Command MSP** and view it next to **Operating System** as shown in the image below:



## Features

**This section highlights major features in nCommand MSP 10.1.1.**

- Added options to the Push Firmware jobs, which can be used to remove all assigned or unassigned existing firmware files from an AOS target device during the Push Firmware job.
- Expanded the capabilities of the filter string search engine.
- Expanded the LLDP data available under the Connected Devices section of a device.
- Added support for the Region assignment of an AOS device, as well as User Region assignment.
- A user can be given server permissions based on their RADIUS authentication results.
- Added support for SNMPv3.

## Fixes

**This section highlights major bug fixes in nCommand MSP 10.1.1**

- Resolved a conflict with AOS which caused a loss of functionality with some AOS devices running AOS versions R12.3.0 or newer.
- Filtering the Devices tab by 'Device Type' for the iterations of TA 908e products produced inaccurate results.
- Corrected an issue preventing some special characters from being used in the local portion of a user's email address.
- An issue could have prevented automatic updates of DeviceDefinition files from being properly installed.
- An issue could have occurred with the Device Alert Overview widget which could have caused it to show an empty list if there were more than 32K alerts to display.
- In rare cases an issue could have arisen for devices which have had a configuration restored through a job, which could have prevented them from being deleted from the server in the future.
- An issue could have prevented Server Alerts from being emailed to a specified user.
- An issue could have caused Firmware Upgrade/Reboot jobs run from a clustered server deployment to fail due to a device communication timeout.
- Selecting the 'Restart' button in the Settings > System Restart menu restarts the server, not just the MSP services. The wording of the text has been changed to clarify that.
- Upgraded OpenSSL software package to address several security concerns.

## Errata

**The following is a list of errata that still exist in nCommand MSP 10.1.1.**

- A user cannot create more than 11 static routes.
- 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 pre-install config jobs).

**Workaround:** Use Internet Explorer.