# Cisco Nexus Dashboard Insights Software Management, Release 6.3.1 - For Cisco NDFC

# Table of Contents

First Published: 2023-09-12

Last Modified: 2023-12-15

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# New and Changed Information

The following table provides an overview of the significant changes up to the current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

*Table 1. New Features and Changed Behavior in the Cisco Nexus Dashboard Insights*

| Feature | Description | Release | Where Documented |
|---|---|---|---|
| Reorganized Content | Content within this document was originally provided in the Cisco Nexus Dashboard Insights User Guide. Starting with release 6.3.1, this content is now provided solely in this document and is no longer provided in the Cisco Nexus Dashboard Insights User Guide. | 6.3.1 | Entire document |

This document is available from your Nexus Dashboard Insights GUI as well as online at www.cisco.com. For the latest version of this document, visit Cisco Nexus Dashboard Insights Documentation.

# Software Management

## Software Management

Before performing an upgrade there are multiple validations that need to be performed. Similarly after an upgrade process, multiple checks helps to determine the changes and the success of the upgrade procedure.

The Software Management feature suggests an upgrade path to a recommended software version and determines the potential impact of upgrade impact. It also helps with the pre-upgrade and post-upgrade validation checks.

The Software Management feature offers the following benefits:

- Assists in preparing and validating a successful upgrade of the network.
- Provides visibility on the pre-upgrade checks.
- Provides visibility on the post-upgrade checks and the status after the upgrade.
- Minimizes the impact to the production environment.
- Provides visibility if the upgrade process is a single step or multiple steps.
- Displays the bugs applicable to a specific firmware version.

### Guidelines and Limitations

Before running a post-upgrade analysis, ensure that all the nodes are already upgraded.

## Software Management Dashboard

Navigate to **Admin** > **Software Management**.

> In general, we recommend that you upgrade to the latest maintenance release and patch for a particular long-lived release. If you need features that were introduced after that release, you can upgrade to the latest release.

The dashboard displays a graph showing the number of jobs along with their status. The table provides the following high-level information about each site:

1. Status
2. Name
3. Site
4. Node Target Firmware
5. Devices
6. Start Time

7. End Time

You can also filter the table based on status. Click the gear icon at the right end of the table header to open a customization window for configuring which columns are displayed in the table.

# Creating Software Management

## Procedure

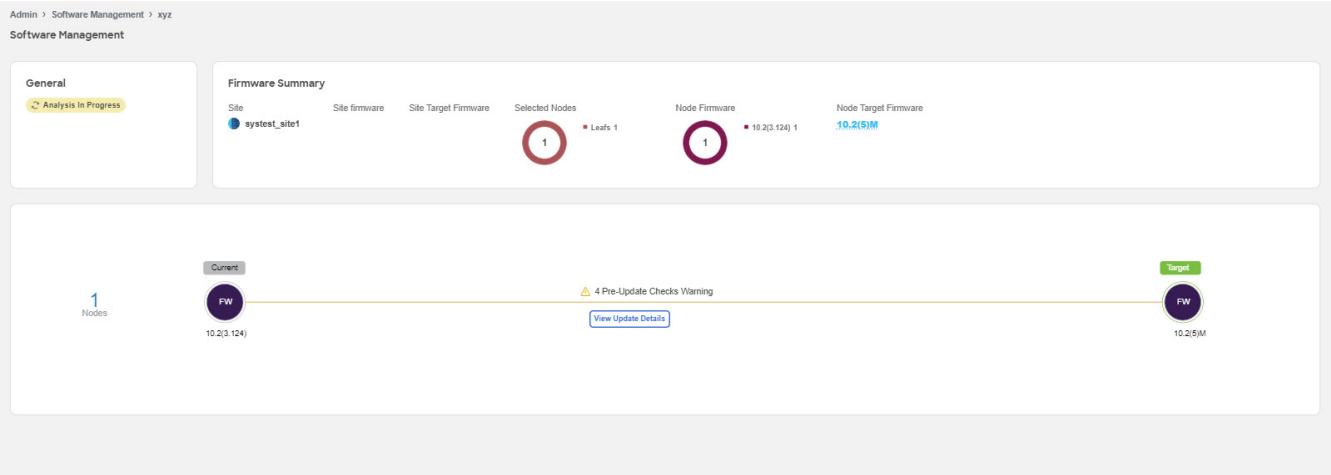
1. Choose **Admin** > **Software Management** > **New Analysis**.
2. Enter the analysis name.
3. Select a site. Click **Next**.
4. Select the firmware. Cisco recommended release and the latest firmware release are displayed.

   > You can also choose to skip this step.

5. Click **Select Nodes**.
   a. Select the nodes. Only the nodes that are required to be updated are displayed. You can only select 10 nodes at a time per analysis.
   b. Click **Add**.
6. Click Create Job. The job is displayed in the **Software Management** Dashboard.
7. Click **View Update Details** to view the pre-update analysis and post update analysis for the firmware or node.

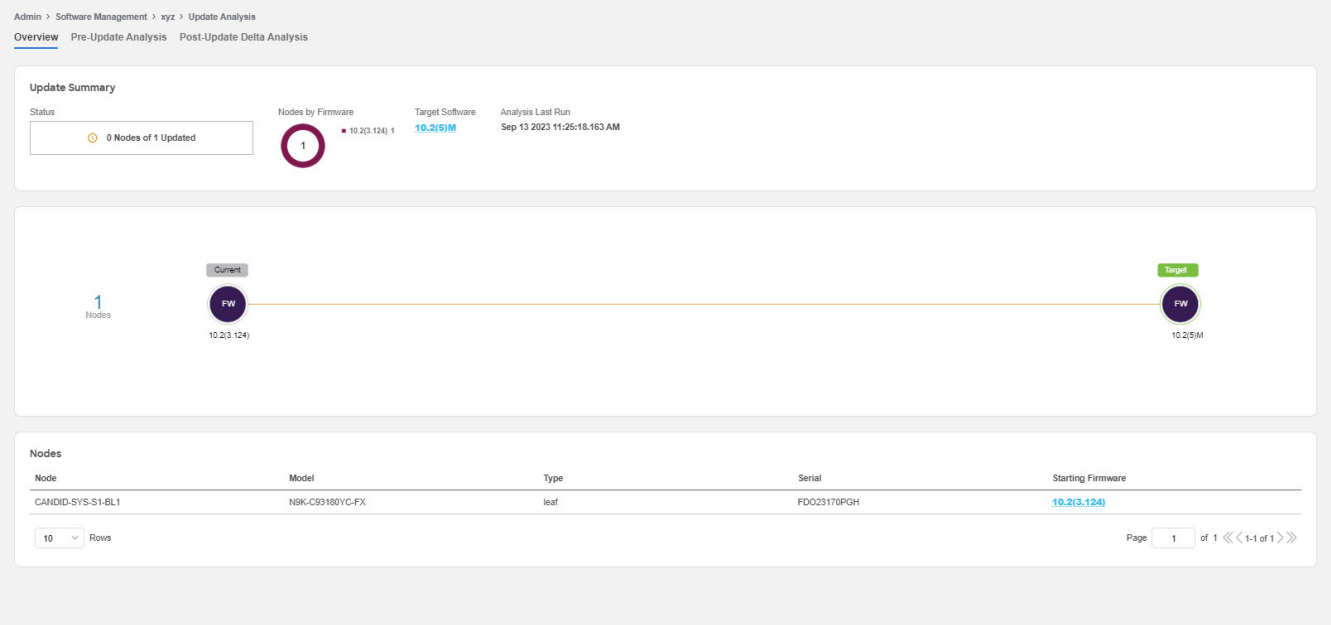
## Analysis Detail

- General - This shows if the analysis status
- Firmware summary - This shows site, site firmware, site target firmware, selected nodes, node firmware and node target firmware
- Upgrade path for the firmware and node. The upgrade path for firmware and node is displayed separately if the firmware is selected.



### *Overview*

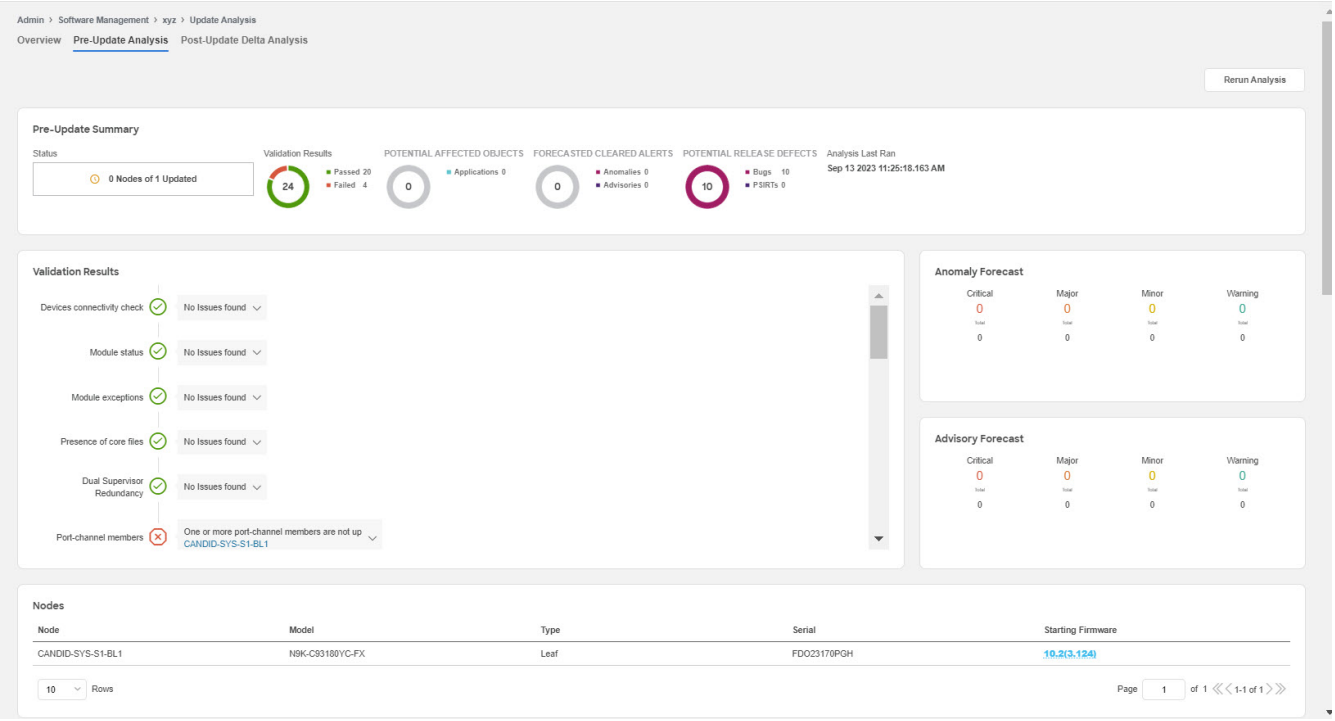
This displays the update summary, the upgrade path and the list of nodes in a tabular form.




### *Pre-Update Analysis*

This displays details such as node status, validation results, potential affected objects, forecasted clear alerts after the upgrade, and potential release defects applicable after the upgrade. This also shows the anomaly and advisory forecast. After fixing any of the issues highlighted in the **Validation Results** area, click **Rerun Analysis**. Click the drop down button to view pre-update validation criteria and the issues detected for each criteria. See Pre-Validation Criteria for NDFC.

We recommend you to run the python script again, upload the file and then run the assurance analysis again to check if the changes had effect on the pre-upgrade validation.



***Post-Update Analysis***

This displays the post-update analysis details. The post-update summary displays the status of the upgrade.

- Click **Health Delta** to view the difference in the anomalies between the pre-upgrade and post-upgrade analysis.
- Click **Operational Delta** to view the difference in the operational resources between the pre-upgrade and post-upgrade analysis.
- Click **Rerun Analysis**.

# Pre-Validation Criteria for NDFC

| Pre-Validation Criteria | Descriptioon | Release |
|---|---|---|
| Could not connect to devices | This validation checks if all devices are connected. | 6.0.1 |
| Check if modules are in ok/active/standby state | This validation checks if all modules are online. | 6.0.1 |
| Found exception log messages in module | This validation checks for non-user initiated resets. | 6.0.1 |
| Found core files on devices | This validation checks for core files. | 6.0.1 |
| Found active supervisor without HA standby | This validation checks the redundancy status on dual supervisor systems. | 6.0.1 |
| One or more port-channel members are not up | This validation checks if all port-channel members are in Up state. | 6.0.1 |
| Found non user-initiated system resets | This validation checks if system reset is due to reasons other than user-initiated. | 6.0.1 |
| Found non user-initiated module resets | This validation checks if module reset is due to reasons other than user-initiated. | 6.0.1 |
| Found modules not in ok state and without backup power | This validation checks if all modules are in ok state and if backup power present. | 6.0.1 |
| Found FAILURE/ABORT/INCOMPLETE/ ErrorDisabled in module | This validation checks for FAILURE/ABORT/INCOMPLETE/ ErrorDisabled results in any module. | 6.0.1 |

| Pre-Validation Criteria | Descriptioon | Release |
|---|---|---|
| Found vPC status is not in Up state | This validation checks if vPC status is in Up state. | 6.0.1 |
| Found vPC sticky bit is false | This validation checks if vPC sticky bit is false. | 6.0.1 |
| Found vPC role is not secondary | This validation checks if vPC role is secondary. | 6.0.1 |
| Found OSPF is in FULL FULL/DR state | This validation checks for OSPF interfaces and process uptime stability (12 hours). | 6.0.1 |
| Found BGP session are not in Up state | This validation checks for BGP neighbors up time stability (12 hours). | 6.0.1 |
| Found HSRP MGO state is not Active/Standby | This validation checks if HSRP MGO state is Active/Standby. | 6.0.1 |
| Found ARPs are in Incomplete state | This validation checks if ARPs are in Incomplete state. | 6.0.1 |
| Not enough free space to continue | This validation checks if bootflash free space is greater than threshold of 5GB. | 6.0.1 |
| Found filesystems with usage higher than 85% | This validation checks if all filesystems usage is equal to or below 85%. | 6.0.1 |
| Found console register bits are not RTS or DTR orDSR | This validation checks if console register bits are RTS or DTR or DSR. | 6.0.1 |
| Found Severity 1, 2 or 3 messages | This validation checks for Severity 1, 2 or 3 messages. | 6.0.1 |
| ISSU impact check was disruptive | This validation checks if ISSU is disruptive or non-disruptive. | 6.0.1 |
| All spines are selected in same upgrade group or no redundant spine available for some nodes | This validation checks if spine nodes are upgraded with at least two separate groups to avoid traffic loss. | 6.0.2 |
| Endpoint network redundancy | This validation checks if nodes have non-redundant connected endpoints to avoid traffic loss during the reboot of nodes. | 6.0.2 |

# Viewing Defect Analysis

## Before you Begin

Ensure that Bug Scan is enabled for all sites.

## Procedure

1. Hover around the starting firmware version or the target software version of a node and click **Defect Analysis** to view the defects associated with the firmware version.
2. Click **Digitized Bug Anomalies** or **Release Noted Defects** to view the details such as type, category, title, description in the table below.
3. Click **Nodes in this version** to view more information on the nodes associated with the firmware version.

In **Defect Analysis**, you can view the bugs, PSIRTs, nodes, and software EOL timeline.

Digitized Bug Anomalies are digitized bugs that are also found as system anomalies in the Bug Scan feature. Release Noted Defects are bugs mentioned as Known Issues in the release notes for a specific firmware version. The software EOL timeline displays the EOL timeline for the firmware version and is color coded based on severity:

- Critical: Red - EOL is less than 90 days from today.
- Warning: Yellow - EOL is between 90 days and 249 days from today.
- Healthy: Green - EOL more than 250 days from today or EOL not yet available and product support is active.

# Copyright