Cisco Nexus Dashboard Insights Software Management, Release 6.3.1 - For Cisco ACI

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 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**

At the top you see the suggested next software version and the latest version available. Using the links, you can view the release notes.

> 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

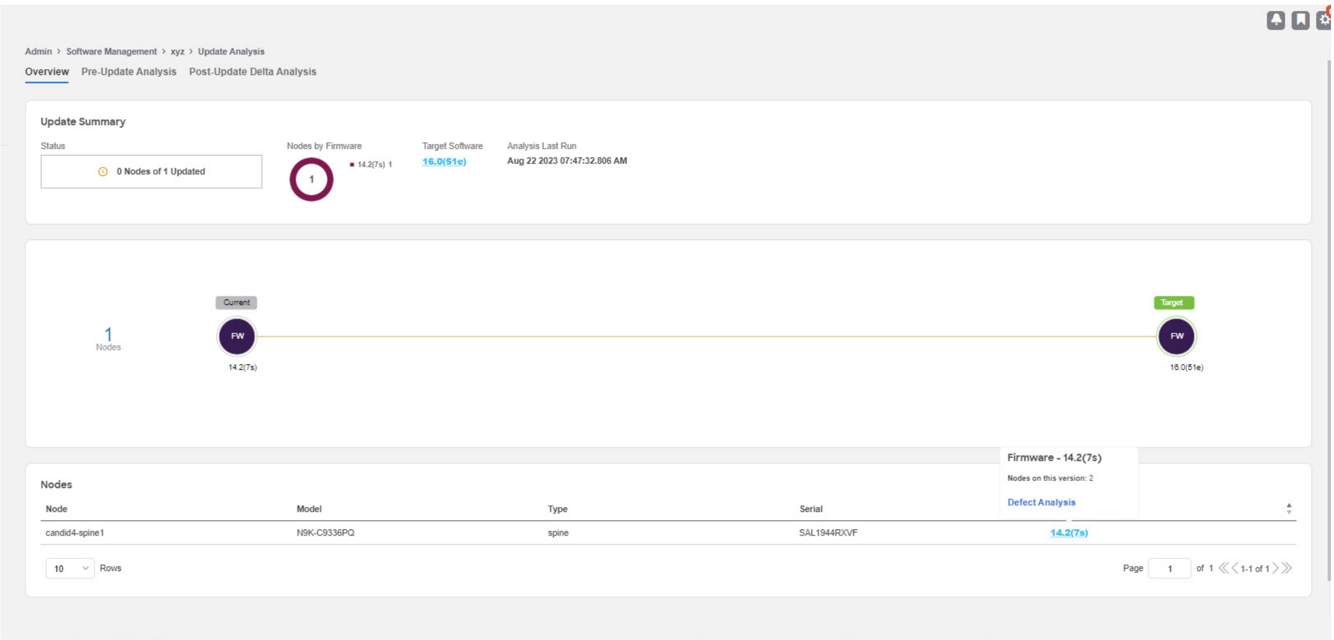
You can also filter the table based on status. Click the gear icon at the right end of the table header to open a customization window for configuring which columns are displayed in the table.

Create Software Management

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 a completed analysis to view the details.



Update Summary

Status: 0 Nodes of 1 Updated

Nodes by Firmware: 1 ■ 14.2(7s) 1

Target Software: 16.0(51e)

Analysis Last Run: Aug 22 2023 07:47:32.806 AM

Nodes

Node	Model	Type	Serial	
candid4-spine1	N9K-C9336PQ	spine	SAL1944RXVF	14.2(7s)

Analysis Detail

- General - This shows if the analysis status
- Firmware summary - This shows site, site firmware, site target firmware, selected nodes, node

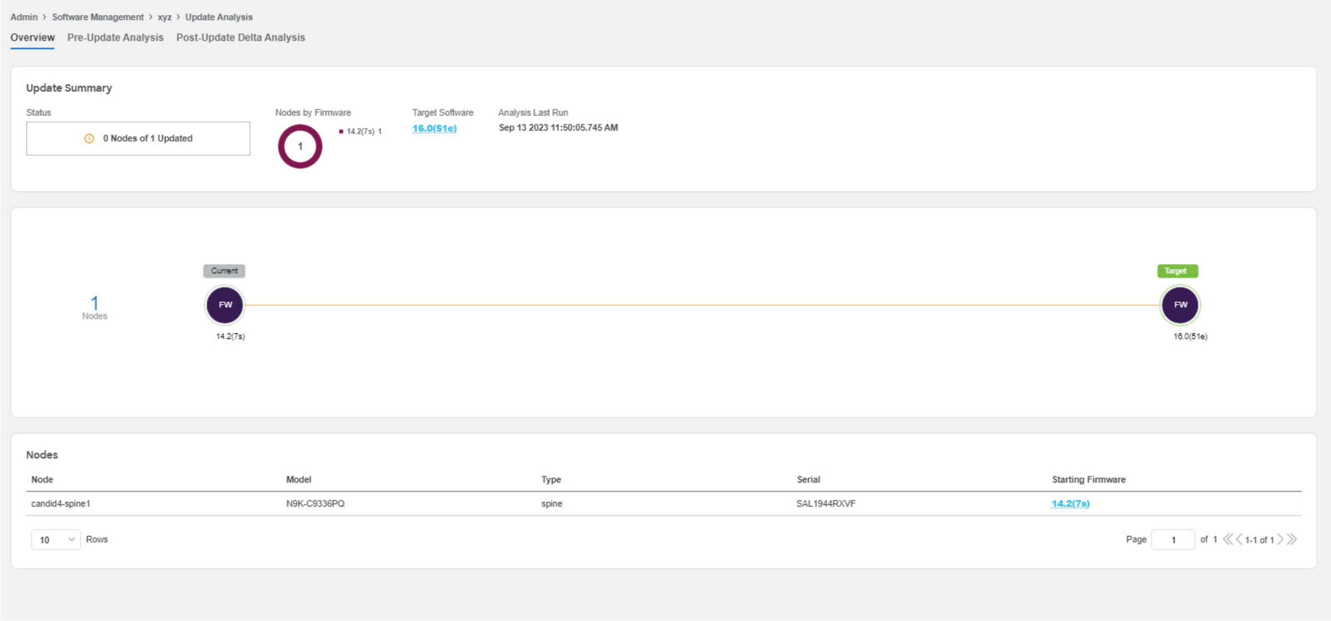
firmware and node target firmware

- Upgrade path for the firmware and node. The upgrade path for firmware and node is displayed separately if the firmware is selected.

Click **View Update Details** to view the pre-update analysis and post update analysis for the firmware or node.

Overview

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



Admin › Software Management › xyz › Update Analysis
Overview
Pre-Update Analysis
Post-Update Delta Analysis

Update Summary

Status: 0 Nodes of 1 Updated

Nodes by Firmware: 14.2(7s) 1

Target Software: 16.0(51e)

Analysis Last Run: Sep 13 2023 11:50:05.745 AM

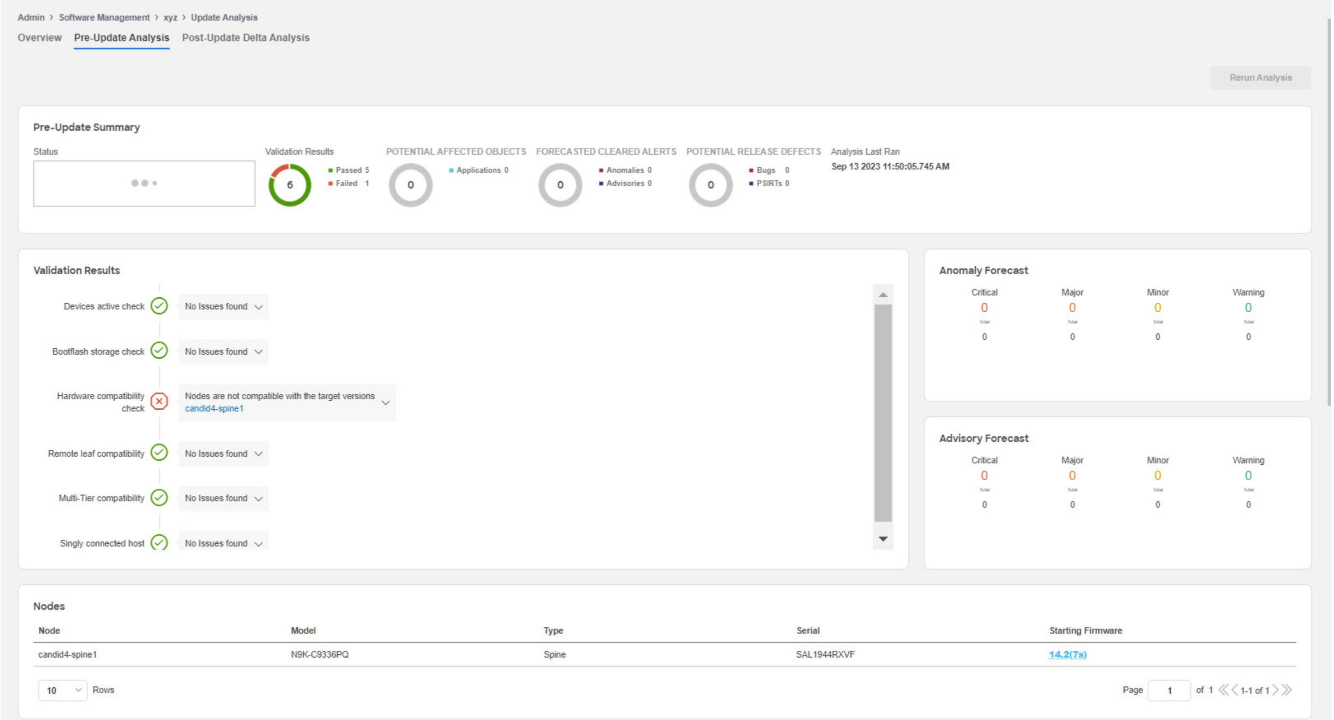
Nodes

Node	Model	Type	Serial	Starting Firmware
candid4-spine1	N9K-C9336PQ	spine	SAL1944RXVF	14.2(7s)

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 Cisco APIC.

> 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.


Admin › Software Management › xyz › Update Analysis
Overview
Pre-Update Analysis
Post-Update Delta Analysis
Rerun Analysis

Pre-Update Summary

Status

Validation Results: 6 — Passed 5, Failed 1

POTENTIAL AFFECTED OBJECTS: 0 — Applications 0

FORECASTED CLEARED ALERTS: 0 — Anomalies 0, Advisories 0

POTENTIAL RELEASE DEFECTS: 0 — Bugs 0, PSIRTs 0

Analysis Last Ran: Sep 13 2023 11:50:05.745 AM

Validation Results

- Devices active check ✓ No Issues found
- Bootflash storage check ✓ No Issues found
- Hardware compatibility check ✗ Nodes are not compatible with the target versions candid4-spine1
- Remote leaf compatibility ✓ No Issues found
- Multi-Tier compatibility ✓ No Issues found
- Singly connected host ✓ No Issues found

Anomaly Forecast

Critical	Major	Minor	Warning
0	0	0	0
Total	Total	Total	Total
0	0	0	0

Advisory Forecast

Critical	Major	Minor	Warning
0	0	0	0
Total	Total	Total	Total
0	0	0	0

Nodes

Node	Model	Type	Serial	Starting Firmware
candid4-spine1	N9K-C9336PQ	Spine	SAL1944RXVF	14.2(7s)

10 Rows   Page 1 of 1 1-1 of 1

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 **Policy Delta** to view the difference in the polices between when the pre-upgrade and post-upgrade analysis were run. This is applicable only for ACI sites.
- Click **Rerun Analysis**.

Pre-Validation Criteria for Cisco APIC

Pre-Validation Criteria	Description	Release
Found inactive devices	This validation checks if all devices are active.	6.0.1
Select a compatible target version	This validation checks if the target firmware version is compatible with the current running version.	6.0.1
Remote leaf compatibility	This validation checks if remote leaf feature is supported in the target firmware version and if the fabric is using remote leaf feature.	6.0.1

Pre-Validation Criteria	Description	Release
Multi-Tier compatibility	This validation check if Multi-Tier topology is supported in the target firmware version and if the fabric has Tier-2 leaf nodes.	6.0.1
The fabric has 4 active critical configuration faults	This validation checks the presence of critical configuration faults or specific faults that may impact the firmware update.	6.0.1
Pod(s) have fewer than two route reflectors for infra MP-BGP	This validation checks if each pod has at least two spine nodes configured as route reflectors for infra MP-BGP.	6.0.1
Nodes are not in vPC	This validation checks if leaf nodes are configured with vPC to ensure the redundancy/high availability during the firmware update.	6.0.1
Nodes do not have out-of-band management IP	This validation checks the presence of nodes without OOB (Out-of-Band) management IP configuration to ensure that you always have access to all nodes.	6.0.1
NTP is not configured	This validation checks if Network Time Protocol (NTP) is configured for Cisco APICs.	6.0.1
Switch upgrade maintenance group check	This validation checks if APICs have maintenance and firmware groups.	6.0.1
Failed to validate rule	This validation checks if the target firmware version is compatible with current running CIMC versions.	6.0.1
Cisco APICs in cluster have different infra VLAN IDs	This validation checks if APICs in the cluster have same infra VLAN IDs	6.0.1
Cisco APIC cluster status is not fully-fit for all APIC nodes	This validation checks if the APIC cluster status is fully-fit for all APIC nodes.	6.0.1

Pre-Validation Criteria	Description	Release
Fabric recovery is in progress	This validation checks if there is any fabric recovery in progress.	6.0.1
The configured SNMPv3 user authorization and/or privacy types are not supported in the target Cisco APIC firmware version	This validation checks if configured SNMPv3 user authorization and/or privacy types are supported in the target APIC firmware version.	6.0.1
Endpoint network redundancy	This validation checks if nodes have non-redundant endpoints to avoid traffic loss during the reboot of nodes.	6.0.2
APIC Cluster Status	This validation checks if the APIC cluster status is fully-fit for all APIC nodes. If it is data-layer-partially-diverged or anything other than fully-fit, firmware update for APICs and switches should not be performed.	6.3.1
APIC Cluster Status	This validation checks if the APIC cluster status is fully-fit for all APIC nodes. If it is data-layer-partially-diverged or anything other than fully-fit, firmware update for APICs and switches should not be performed.	6.3.1
APIC Disk Space	This validation checks if there are any faults warning that an APIC is running low on disk space. This could cause the APIC upgrade to fail. APICs raise three different faults depending on the amount of disk space remaining. If any of these faults are raised on the system, the issue should be resolved prior to performing the upgrade.	6.3.1

Pre-Validation Criteria	Description	Release
Switch Bootflash Usage	This validation checks if there is enough bootflash storage to successfully upgrade a switch node.	6.3.1
APIC SSD Health	This validation checks if there are any faults warning the APIC SSD health status.	6.3.1
Switch SSD Health	This validation checks if there are any faults warning the Switch SSD health status.	6.3.1
Daily Configuration Backup	This validation checks if there is a valid configuration backup taken in the last 24 hours.	6.3.1
NTP Configuration	This validation checks if Network Time Protocol (NTP) is configured for APICs.	6.3.1
NTP Status	This validation checks if Network Time Protocol (NTP) is Synced on APICs and Switches in the Fabric.	6.3.1
OOB management IP	This validation checks the presence of nodes without OOB (Out-of-Band) management IP configuration to ensure that you always have access to all nodes. During the upgrade/downgrade, nodes may not be reachable via ACI infra. It is recommended to prepare console access to each node as well just in case.	6.3.1
Ongoing Fabric Recovery	This validation checks if there is any fabric recovery in progress.	6.3.1
Active Apps	This validation checks if there are any active apps in the APIC that need to be disabled.	6.3.1
Configuration Zones	This validation checks if there are any configuration zones that need to be disabled or removed prior to the upgrade.	6.3.1

Pre-Validation Criteria	Description	Release
Switch High Availability (vPC Leafs)	This validation checks if leaf nodes are configured with vPC to ensure the redundancy/high availability during the firmware update. If the fabric provides redundancy via other means such as ECMP, or has single-homed servers on purpose, ignore this check.	6.3.1
Switch High Availability (Spine Route Reflectors)	This validation checks if each pod has at least two spine nodes configured as route reflectors for infra MP-BGP. If all route reflector spine nodes are unavailable at the same time, the fabric will lose the reachability to external routes from L3Outs.	6.3.1
Upgrade Group (Spine HA)	If any maintenance groups are found, this validation checks for 1) Not all spines in the same pod are upgraded in the same group. 2) Not all BGP Route Reflector spines are upgraded in the same group. 3) Not all IPN/ISN spines are upgraded in the same group.	6.3.1
Upgrade Group (vPC HA)	This validation checks that both leaf nodes of the same vPC pair are not in the same upgrade group.	6.3.1
Upgrade Group (APIC Leaf HA)	This checks that both leaf nodes connected to the same APIC do not belong to the same upgrade group.	6.3.1

Pre-Validation Criteria	Description	Release
Critical Configuration Faults	This validation checks the presence of critical config faults or specific faults that may impact the firmware update.	6.3.1
Controller Port Configuration Conflict	This validation checks if there are any faults warning that there is configuration being rejected because it’s deployed on an APIC connected port.	6.3.1
L3 Interface Deployment Conflict	This validation checks if there are any faults warning that L3 configuration is being rejected on a port already operating in L2 mode.	6.3.1
L2 Interface Deployment Conflict	This validation checks if there are any faults warning that L2 configuration is being rejected on a port already operating in L3 mode.	6.3.1
Overlapping BD Subnets	This validation checks if there are any faults warning that BD subnets are not the same but overlapping in the same VRF. Only one of those configurations takes effect at a given time. Hence, after the upgrade, a different BD subnet than before may take effect.	6.3.1
Duplicated BD Subnets	This validation checks if there are any faults warning that external Bridge Domains in the same VRF have overlapping prefixes.	6.3.1
External EPG Prefix Overlap	This validation checks if there are any faults warning that external EPGs in the same VRF have overlapping prefixes.	6.3.1
HW Programming Failure (L3Out Prefixes, Contracts)	This validation checks if there are any faults warning that L3Out prefix to pcTag mapping entries or contracts are failed to be programmed.	6.3.1

Pre-Validation Criteria	Description	Release
Scalability (Faults Related to Capacity Dashboard)	This validation checks if there are any stats faults (TCA: Threshold Crossing Alert) related to object eqptcapacityEntity warning scalability issues that can be checked via Capacity Dashboard in the APIC GUI. By default, not all stats in Capacity Dashboard are configured with thresholds to raise a fault. This can be checked and configured under Fabric > Fabric Policies > Policies > Monitoring > default > Stats Collection Policies > Monitoring Object > Equipment Capacity Entity (eqptcapacityEntity) > Stats Type.	6.3.1
Overlapping VLAN Pools	This detects VLAN pools with overlapping VLAN IDs on the same EPG. Such configuration may cause traffic impact after or during an upgrade unless this configuration is intentional and you are familiar with how VNIDs are assigned and work in ACI.	6.3.1
ISIS Redistribution Metric for Multi-Pod/Multi-Site	This checks ISIS redistribution metrics for multi-pod and multi-site.	6.3.1
L3Out MTU Size	This validation checks the MTU size configured on all Layer 3 Outs in the Fabric. If the MTU size on ACI L3Out sides and connected devices does not match, route-exchange after an upgrade may fail even if everything used to work prior to the upgrade.	6.3.1

Pre-Validation Criteria	Description	Release
Different Infra VLAN via LLDP	This validation checks if there are any faults. If you have interfaces connected back-to-back between two different ACI fabrics, you must disable LLDP on those interfaces prior to upgrades. This is because when the switch comes back up after the upgrade, it may receive and process LLDP packets from the other fabric that may be using a different infra VLAN. If that happens, the switch incorrectly tries to be discovered through the infra VLAN of the other fabric and will not be discoverable in the correct fabric.	6.3.1
Offline VMM Domain	This validation checks if any VMM Domains have controllers which are offline.	6.3.1
VMM Domain LLDP/CDP Adjacency	This validation checks if there are any faults warning when APIC cannot find LLDP/CDP information of vSwitch through vCenter for VMM DVS integration. The LLDP/CDP information is used to detect which interfaces of ACI switches to deploy VLANs dynamically.	6.3.1
CIMC compatibility	This validation checks if the target firmware version is compatible with current running CIMC versions.	6.3.1
Version compatibility	This validation checks if the target firmware version is compatible with the current running version.	6.3.1

Pre-Validation Criteria	Description	Release
Remote leaf compatibility	This validation checks if remote leaf feature is supported in the target firmware version if the fabric is using remote leaf feature. This check is mainly for downgrade scenario.	6.3.1
Multi-Tier compatibility	This validation check if Multi-Tier topology is supported in the target firmware version if the fabric has Tier-2 leaf nodes. This check is mainly for downgrade scenario.	6.3.1
Switch upgrade maintenance group check	This validation checks if APICs have Maintenance and Firmware groups exists before upgrade from pre-4.0 to 4.0 or later releases.	6.3.1
Infra VLAN ID check	This validation checks if APICs in the cluster have same infra VLAN IDs.	6.3.1
SNMPv3 auth compatibility	This validation checks if configured SNMPv3 user authorization and/or privacy types are supported in the target APIC firmware version.	6.3.1

Viewing Defect Analysis

Before you Begin

Ensure that Bug Scan is enabled for all sites.

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