Caveats

Caveats describe unexpected behavior in a product. The Open Caveats section lists open caveats that apply to the current release and may apply to previous releases. A caveat that is open for a prior release and is still unresolved applies to all future releases until it is resolved.

To view the details of the software bugs pertaining to your product, perform the following task:

- Click the Caveat ID/Bug ID number in the table.

The corresponding **Bug Search Tool** window is displayed with details of the Caveat ID/Bug ID.

The Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data, such as bug details, product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat whose ID you do not have, perform the following procedure:

1. Access the BST using your Cisco user ID and password at:

   https://tools.cisco.com/bugsearch/

2. In the **Bug Search** window that is displayed, enter the necessary information in the corresponding fields.

For more information about how to use the Cisco Bug Search Tool effectively, including how to set email alerts for bugs and to save bugs and searches, see Bug Search Tool Help & FAQ.

This chapter lists the Open and Resolved Caveats in Cisco DCNM, and contains the following section:

Cisco DCNM, Release 10.4(2)

Resolved Caveats

The following table lists the Resolved bugs for Cisco DCNM, Release 10.4(2).

Caveat ID Number	Description
CSCvg32790	Native HA validation for Active/Standby on different subnets.

Caveat ID Number	Description
CSCvg41098	Upgrading 10.2(1) OVA federation to 10.4(1)—AMQP is not starting automatically or manually.
CSCvg51299	HTTP to HTTPS redirection is blocked in Cisco DCNM 10.4(1).

Open Caveats

The following table lists the Open bugs for Cisco DCNM, Release 10.4(2).

Caveat ID	Description
CSCvg46901	PMN-INTEROP:Issue when DCNM discovers PIM Router.
CSCvf99030	Deleting network is deleting VRF as well
CSCvg76382	Role change of leaf to BL with some vrfs deployed
CSCvg76798	Multisite: BGW loopback0 , loopback1 need to have 'tag 54321' configured
CSCvb40889	Unable to edit the default L2 L3 segment IDs in LAN fabric
CSCvg87498	NFM Migration: Handling of switch reload while Migration in progress
CSCvg39897	Nexus 9504 should show only the physical / loopback interfaces in Cisco DCNM
CSCvg87251	The **appmgr change_pwd ssh root** command thows error though it is changing the root password
CSCvg91823	Topdown: RMA of the devices after top-down deployment
CSCvg93573	Topology View doesnt show FEX uplink connections
CSCvh13788	When you upgrade to DCNM release 10.4(2), temperature data will not be backed up automatically as part of the appmgr backup script on an OVA/ISO setup where EPL is not enabled.
CSCvg76382	If there are VRFs and/or networks deployed to a Nexus 9000 switch in a VXLAN BGP EVPN network via the top-down fabric provisioning mechanism, then a role change for that switch (Border to leaf or vice-versa) may cause subsequent deployments or modifications to existing deployments, to fail.
CSCvi37845	Alarm log files keep on incremeting in the /usr/local/cisco/dcm/fm/log folder.