



## 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 page 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 the Bug Search Tool Help & FAQ page [Bug Search Tool Help & FAQ](#).

This chapter lists the Open and Resolved Caveats in Cisco Prime Data Center Network Manager (DCNM), Release 7.1:

- [Cisco Prime DCNM, Release 7.1\(2\), Caveats, page 2](#)
- [Cisco Prime DCNM, Release 7.1\(1\), Caveats, page 3](#)

# Cisco Prime DCNM, Release 7.1(2), Caveats

## Resolved Caveats

The following table lists the Resolved bugs for Cisco Prime DCNM, Release 7.1(2).

Bug ID	Headline
<a href="#">CSCuo31949</a>	Admin >logs >web reports not showing logs for executed reports.
<a href="#">CSCus02931</a>	WebUI: Health->vpc displays n/a for vpc leg fex port channel.
<a href="#">CSCus03320</a>	SME Web Client Host Section Not Displaying Host Info Resulting Error.
<a href="#">CSCus27527</a>	December 2014 - NTPd.org Vulnerabilities.
<a href="#">CSCus77553</a>	DCNM 7.1.1 - Can not delete zone from zone set

## Open Caveats

The following table lists the Open bugs for Cisco Prime DCNM, Release 7.1(2).

Bug ID	Headline
<a href="#">CSCul88797</a>	Connection between Fex and N1k not shown for 2 layer vPC.
<a href="#">CSCuo15884</a>	Topology view: Incorrect Discovery Port.
<a href="#">CSCus87367</a>	Upgraded dcnm from 7-0-2 to 7-1-1-32S0 and reports from 702 are not there.
<a href="#">CSCus87435</a>	Upgraded dcnm from 7-0-2 to 7-1-1-103 and LDAP auth not working anymore.
<a href="#">CSCut13133</a>	SAN client summary E/TE port count matches with web client dashboard.
<a href="#">CSCut78596</a>	Upgraded dcnm from 7-0-2 to 7-1-1-103 -not able to https as before upgd.
<a href="#">CSCut81564</a>	Edit SMIS provider window doesnt show by which server array is managed.
<a href="#">CSCut82082</a>	SAN client launch "DCNM server" field issue OVA setup.

Bug ID	Headline
<a href="#">CSCut94618</a>	SSL certificate is not retained after upgrade.
<a href="#">CSCuu08302</a>	Errors seen in Restore script.
<a href="#">CSCuu15585</a>	DCNM (106) xmpp failed to add device in case of using selective-HA.

## Cisco Prime DCNM, Release 7.1(1), Caveats

### Resolved Caveats

The following table lists the Resolved bugs for Cisco Prime DCNM, Release 7.1(1).

Bug ID	Headline
<a href="#">CSCuf73759</a>	Discovering setup for two layer vpc one by one.
<a href="#">CSCuo18159</a>	NPV Setup Wizard shows error while enabling NPV.
<a href="#">CSCup75509</a>	TACACS & Radius auth for WebUI login failing, but LAN & SAN login working.
<a href="#">CSCun86190</a>	POAP template: modify value for array type parameter not taking effect.
<a href="#">CSCur48635</a>	Multi-role LDAP authentication on DCNM fails.
<a href="#">CSCus00241</a>	Cisco DCNM FileServlet Information Disclosure Vulnerability.

### Open Caveats

The following table lists the Open bugs for Cisco Prime DCNM, Release 7.1(1).

Bug ID	Headline
<a href="#">CSCul88797</a>	Connection between Fex and N1k not shown for 2 layer vPC.
<a href="#">CSCuo15884</a>	Topology view: Incorrect Discovery Port.
<a href="#">CSCuo31949</a>	Admin >logs >web reports not showing logs for executed reports.
<a href="#">CSCus02931</a>	WebUI: Health->vpc displays n/a for vpc leg fex port channel.

Bug ID	Headline
<a href="#">CSCus03320</a>	SME Web Client Host Section Not Displaying Host Info Resulting Error.
<a href="#">CSCus77553</a>	DCNM 7.1.1 - Can not delete zone from zone set