



## Caveats

---

- [Bug Search Tool](#), on page 1
- [Resolved Caveats](#), on page 2
- [Open Caveats](#), on page 2

## Bug Search Tool

The system grades known problems (bugs) per severity level. These release notes contain descriptions of the following bug levels:

- All severity level 1 or 2 bugs
- Significant severity level 3 bugs
- All customer-found bugs

You can search for open and resolved caveats of any severity for any release using the Cisco Bug Search tool, an online tool available for customers to query defects according to their own needs.

To access the Cisco Bug Search tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

Follow these steps to use Cisco Bug Search tool:

1. Access the Cisco Bug Search tool: <https://tools.cisco.com/bugsearch/>.
2. Log in with your Cisco.com user ID and password.
3. If you are looking for information about a specific problem, enter the bug ID number in the **Search for:** field and click **Go**.



---

**Tip** Click **Help** on the Bug Search page for information about how to search for bugs, create saved searches, and create bug groups.

---

## Resolved Caveats

The following table lists severity 1, 2, and 3 defects that are resolved for Cisco Prime License Manager 11.5(1)SU7. For more information about an individual caveat, click the Identifier.

You must be a registered Cisco.com user to access this online information. Because a caveat's status continually changes, this table only reflects a snapshot of the caveats that were resolved at the time this report was compiled. For an updated view of resolved caveats, access Bug Toolkit - <https://tools.cisco.com/bugsearch>.

*Table 1: Resolved Caveats for Cisco Prime License Manager 11.5(1)SU7*

Identifier	Headline
<a href="#">CSCvq97227</a>	Cisco Prime License Manager Unauthorized Password Reset Vulnerability

## Open Caveats

There are no known issues in this release.